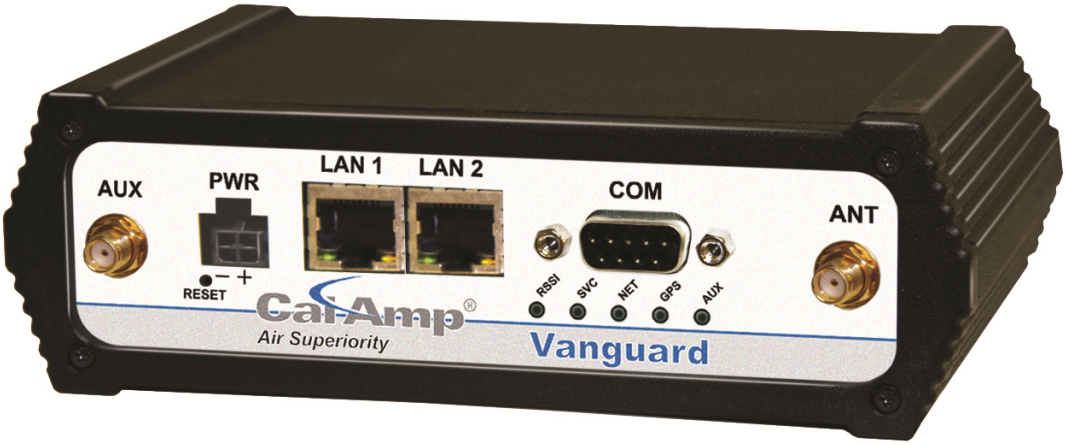
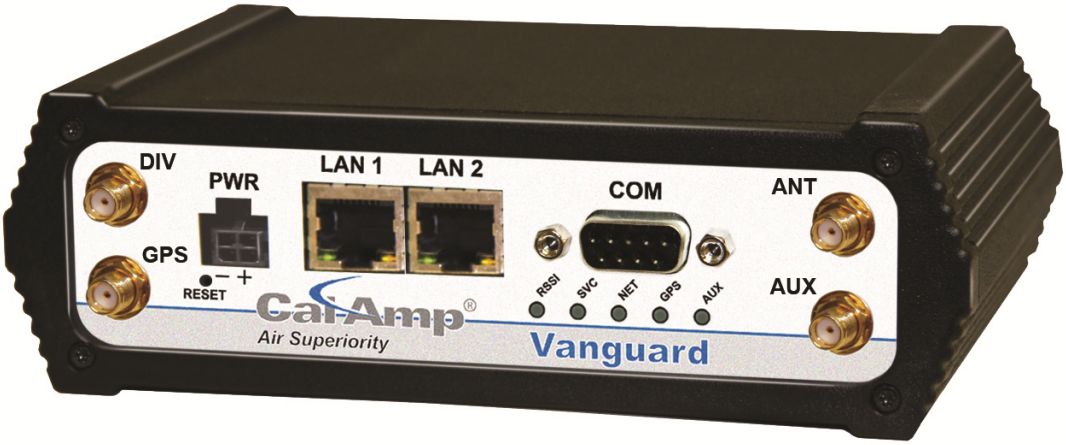
USATCORP.COM

Contact USATCORP.COM for more information or quantity pricing

1-888-550-8728

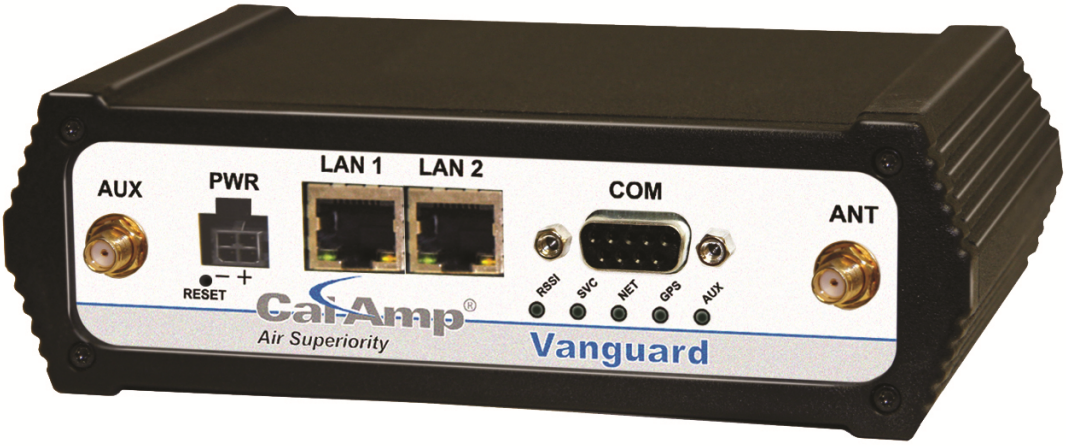


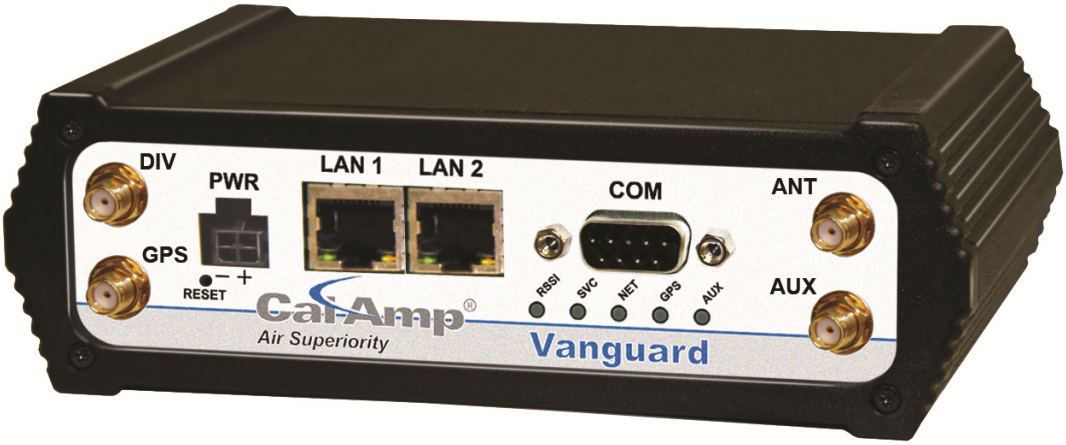


CalAmp

Vanguard Cellular Data Modem & IP Router Series

User Manual
001-7200-100
Revision 0; June 2011





CalAmp

Vanguard Cellular Data Modem & IP Router Series

User Manual
001-7200-100
Revision 0; June 2011

Copyright Notice
©2011 CalAmp. All Rights Reserved.

CalAmp reserves the right to modify the equipment, its specification or this manual without prior notice, in the interest of improving performance, reliability, or servicing. At the time of publication all data is correct for the operation of the equipment at the voltage and/or temperature referred to. Performance data indicates typical values related to the particular product.

No part of this documentation or information supplied may be divulged to any third party without the express written consent of CalAmp. Products offered may contain software which is proprietary to CalAmp. The offer or supply of these products and services does not include or infer any transfer of ownership.

Modem Use
The Vanguard Series modems are designed and intended for use in fixed and mobile applications. “Fixed” assumes the device is physically secured at one location and not easily moved to another location. Please keep the cellular antenna at a safe distance from your head and body while the modem is in use.

Important
Maintain a distance of at least 20 cm (8 inches) between the transmitter’s antenna and any person while in use. This modem is designed for use in applications that observe the 20 cm separation distance.

Interference Issues
Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action or both.
- Do not operate in the vicinity of gasoline or diesel-fuel pumps unless use has been approved and authorized.
- Do not operate in locations where medical equipment that the device could interfere with may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

Mobile Application Safety

- Do not change parameters or perform other maintenance of the 882 GSM Series modem while driving.
- Road safety is crucial. Observe National Regulations for cellular telephones and devices in vehicles.
- Avoid potential interference with vehicle electronics by correctly installing the 882 GSM Series modem. CalAmp recommends installation by a professional.

Revision History

2011 June	Initial Release

Table of Contents

1 Product Overview 6
1.1 Module Identification 6
1.2 Features and Benefits 6
1.3 General Specifications 7
1.4 Mechanical Specifications 8
1.5 Order Informaiton 8
1.6 External Connectors 10
1.7 Antenna 11
1.8 RS-232 Serial Port Integration Parameters 12
1.8.1 ODP (Open Developers Platform) over RS-232 12

2 Getting Started 13
2.1 Package Contents 13
2.2 Device Connections 13
2.3 LAN Configuration 13
2.4 Cellular connections 14
2.4.1 GSM Users 14
2.4.2 CDMA Users 14

3 Vanguard Web Interface 15
3.1 Unit Status 15
3.1.1 Status 15
3.1.2 Basic Settings 20
3.2 SIM Settings (GSM MODELS ONLY) 21
3.2.1 Enabling PIN Security 21
3.2.2 PIN security options 22
3.3 Provisioning (CDMA MODELS ONLY) 24
3.3.1 Verizon Wireless provisioning Information (OTASP) 24
3.3.2 Sprint provisioning information (OMA-DM) 24
3.3.3 Advanced Settings 27
3.4 Cell Connection 29
3.4.1 Dial Settings 29
3.4.2 System Monitor 31
3.4.3 Dynamic DNS 34
3.5 LAN Settings 35
3.5.1 MAC Filtering 39
3.6 Router 40
3.6.1 Port Forwarding 40
3.6.2 Static Routes 42
3.7 VPN 43
3.7.1 PPTP 44
3.7.2 IPSec 45
3.7.3 GRE 48
3.8 Serial 49
3.8.1 External Serial 49
3.8.2 Internal Serial 54
3.9 Diagnostics 55
3.9.1 SNMP 55
3.9.2 Logging 57
3.10 I/O Settings 58

3.10.1 Status 58
3.10.2 Settings 60
3.10.3 Labels 61
3.11 Firmware Update 62

4 Service and Support 65

Appendix A – Abbreviations 66
Appendix B – Warranty Statement 67

1 PRODUCT OVERVIEW

The Vanguard Series from CalAmp is the ideal solution for a wide range of cellular data network serial and Ethernet connectivity requirements.

CDMA models feature EV-DO Rev A speeds with data rates up to 3.1 Mbps downlink and 1.8 Mbps uplink and are backward compatible to EV-DO Rev 0 and 1xRTT dependant on carrier service availability. This occurs automatically to the level of service available. Dual Band Digital CDMA 800 MHz and CDMA PCS 1900 MHz models supports packet-switched services.

GSM models feature Tri-Band UMTS/HSUPA (850/1900/2100) and Quad-Band GSM/GPRS network support with data rates up to 7.2 Mbps downlink and 2.0 Mbps uplink for HSPA and are backwared compatible to HSUPA, HSDPA, EDGE and GPRS dependent on carrier service availability.

1.1 MODULE IDENTIFICATION

The module identification label can be found on the bottom of your Vanguard device. This label contains the product part number, the serial number, FCC and IC IDs as well as carrier specific information that will be required when activating your data account.

CDMA module identification labels contain the device ESN numbers. This number is required by your cellular carrier when activating your data contract. The ESN number is provided in both decimal and Hex formats. The format required for activation is carrier dependent.

GSM module identification lables contain an International Mobile Equipment Identity (IMEI) number shown in decimal format. This number is used by the GSM network only to identify and validate the device. It has no permanent or semi-permanent relation to the subscriber.

Figure 1 CDMA Module Idenficiation Label

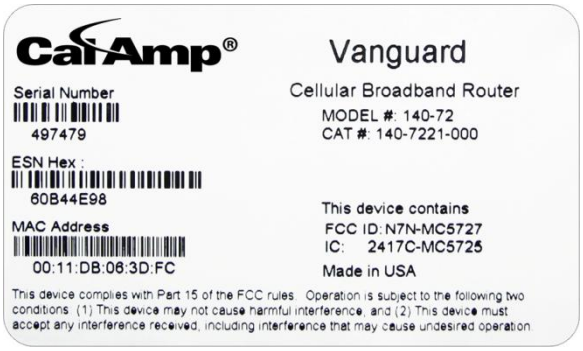
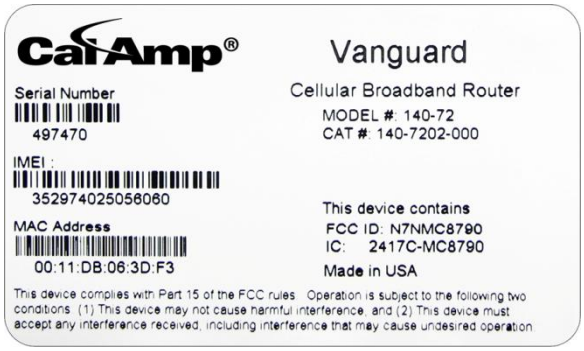

CalAmp®
Vanguard
Cellular Broadband Router
Serial Number
497479
MODEL #: 140-72
CAT #: 140-7221-000
ESN Hex :
60B44E98
This device contains
FCC ID:N7N-MC5727
IC: 2417C-MC5725
MAC Address
00:11:DB:06:3D:FC
Made in USA
This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Figure 2 GSM Module Idenficiation Label


CalAmp®
Vanguard
Cellular Broadband Router
Serial Number
497470
MODEL #: 140-72
CAT #: 140-7202-000
IMEI :
352974025056060
This device contains
FCC ID: N7NMC8790
IC: 2417C-MC8790
MAC Address
00:11:DB:06:3D:F3
Made in USA
This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

1.2 FEATURES AND BENEFITS

- Supports Dynamic or Static IP
- Inbound and Outbound Ethernet Routing
- DHCP Server and Inbound port mapping/translation (Port Forwarding)
- Firewall configuration for increased network security
- Diversity antenna port/auxiliary port for increased receive sensitivity
- Local or remote configuration using HTML web server

- TCP/IP Packet assembler and dis-assembler for serial connected devices
- Inbound IP termination with Static IP
- Modem Domain Names with Dynamic DNS
- Embedded Linux on ARM 9 processor
- Internet access and web browsing via Ethernet connector
- VPN support
- On-board 1.8/3V SIM socket (Active only for GSM Models)

1.3 GENERAL SPECIFICATIONS

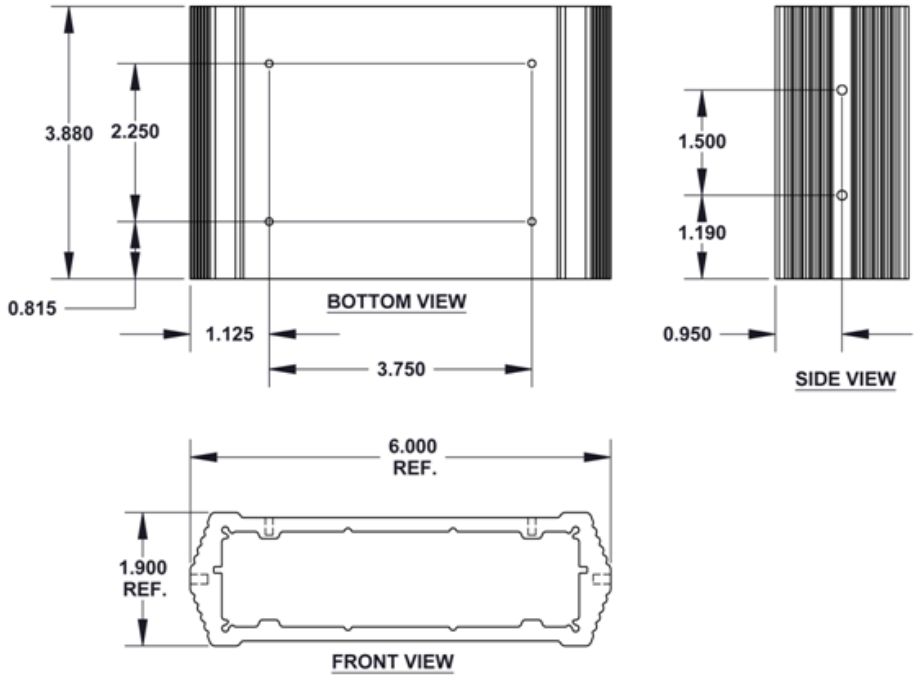
Product specifications are subject to change without notice.

Interface Connectors	RS-232 DE-9S Connector (DCE female) 10/100 Base-T Full Duplex (Dual) 10 Pin I/O Port USB Client port
Power Connector	Molex 43045-4000 MicroFit 3.0, 4 pin header
LED Indicators	RSSI, SVC, NET, GPS, AUX
Antenna Interface	Primary Antenna 50-ohm SMA Female Diversity Antenna 50-ohm SMA Female GPS Antenna 50-ohm, 3.3V SMA Female WiFi Antenna 50-ohm RP-SMA Plug
Size	4.5 (L) x 6.0 (W) x 1.9(H) inches (11.4 x 15.2 x 4.8 cm)
Weight	1.94lb (0.88 kg)
Power Input	9-28 VDC
Maximum TX Power	CDMA 25 dBm GSM/EDGE 33 dBm UMTS 24 dBm
Rx Sensitivity	CDMA >-107 dBm GSM/EDGE >-105 dBm UMTS >-109 dBm
Frequencies	Cellular: TX: 824-849 MHz; Rx: 869-894 MHz PCS: TX: 1850-1910 MHz; Rx: 1930-1990 MHz
Temperature	Operating: -30°C to +70°C 100% duty cycle. *Note: Cellular TX power may be reduced outside this range;* Storage: -40° to +85°C (-40° to +185°F)
Emissions	FCC Part 15b
Transport Protocols	UDP/TCP
Command Protocol	Web Interface

1.4 MECHANICAL SPECIFICATIONS

The following section describes in detail the exterior dimensions of the 882 GSM Series modems and how to utilize the mounting flanges to secure the modem to any surface, which can be drilled for such a purpose. The drawings may be used as layout reference, but it is advised that a physical comparison be made to the modem before proceeding with the mounting process.

Figure 3 Vanguard Mechanical Drawing



1.5 ORDER INFORMAITON

Table 1 shows the available order options and the part numbers required for ordering Vanguard modems.

Table 1 - Vanguard Order Information

	Carrier Options	STANDARD MODELS	ADD GPS	ADD GPS + WI-FI
EVDO	VERIZON	140-7221-000	140-7221-010	140-7221-110
EVDO	SPRINT	140-7223-000	140-7223-010	140-7223-110
EVDO	BELL MOBILITY	140-7225-000	140-7225-010	140-7225-110
HSPA	AT&T	140-7202-000	140-7202-010	140-7202-110
HSPA	TELSTRA	140-7207-000	140-7207-010	140-7207-110
HSPA	GSM CARRIERS	140-7206-000	140-7206-010	140-7206-110

Table 2 - Vanguard Accessories

Vanguard Accessories

	ACC-ANTN-RBD 4” Rubber Duck Antenna
	ACC-ANTN-MAG 3” Mag Mount Antenna
	ACC-PWSP-ML2 110 VAC Input Power
	ACC-PWDC-MLX DC Power Cable
	ACC-CABL-SER DB-9 Serial Cable
	ACC-CABL-ETH 7’ Ethernet cable

1.6 EXTERNAL CONNECTORS

This section describes the external connectors for the Vanguard modem.

- Figure 4 shows the front panel connections for Standard (Fixed) models.
- Figure 5 shows the front panel connections for Mobile models with GPS and WiFi.
- Figure 6 shows the rear panel for all models.
-

- Table **3** describes these connections.

Figure 4 Front Panel Standard Models

Figure 5 Front Panel Mobile Models with GPS and WiFi

Figure 6 Rear Panel Connections

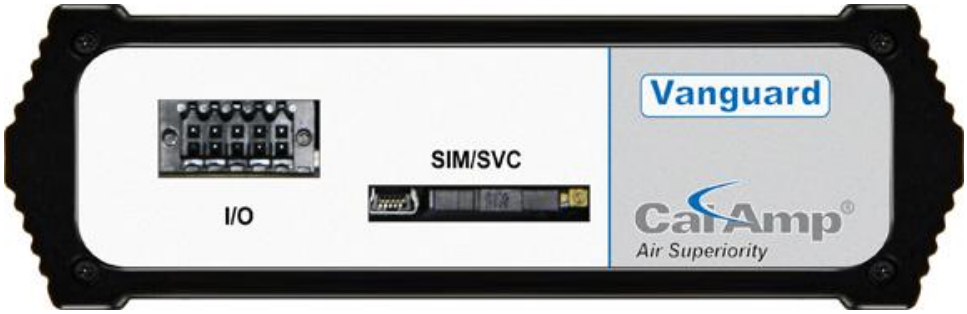


Table 3 – External Connectors

Panel Indicator	Connection	Description
COM	RS-232	Serial to IP conversion use
ANT	SMA	Primary RF Antenna
AUX (Figure 4)	SMA	Cellular Diversity or Cellular/GPS combination antenna
AUX (Figure 5)	RP-SMA	Wi-Fi antenna
GPS	SMA	GPS Antenna
DIV	SMA	Cellular Diversity Antenna
LAN 1, LAN 2	RJ-45	Interface for Ethernet connection to devices
SIM/SVC	USB Mini	Available for CalAmp Support Use Only
RESET		Hold for one second to reset unit. If held for at least 4 sec, unit will reconfigure to factory default settings.
PWR Jack	Molex 43025-0400; Power – bottom pins; I/O – top pins	Interface for power plug (9-28VDC) Interface for Input and Output control lines; ODP use only.
SIM/SVC	SIM Card socket	Interface for SIM card. Your wireless service provider will supply the SIM card with your wireless service contract.

Table 4 – Status LEDs

Function	Off	Green	Flash Green	Red	Flash Red	Amber	Flash Amber
RSSI		Strong		Weak/None		Medium	
SVC		3G	3G/NC		NC	2G	2G/NC
NET	No Connectivity		RX Data		TX Data		RX/TX
GPS	Disabled	Fix	Search	No Fix			
Aux	Disabled	Good		Failed			

- If SVC is solid, then modem is connected to internet. If flashing, the modem is trying to connect to the network.
- Net indicates direction of data.
- Aux refers to WiFi in mobile models.

The LEDs act different than the table at boot. The boot sequence is: All Red, All Amber, All Green, All Flash Green 3 times. Boot sequence is complete.

1.7 ANTENNA

Primary antenna connections are SMA female connectors and must be used with antenna with SMA male connectors. When using a direct mount or rubber duck antenna, choose the antenna specific to your band requirements. Mounting options and cable lengths are user's choice and application specific.

The AUX antenna connector is installed on all standard models and can be used for Diversity or True GPS. The diversity port supports three bands, Cellular (850 MHZ), PCS(1900 MHZ), and GPS(1575 MHZ). Connect a dual band cellular antenna to this port to implement RX diversity on the unit and increase receive sensitivity on the cellular network. Connect a GPS

antenna, with an average gain >-5dBi, if using the GPS functionality. If both RX diversity and GPS are required, install a Cellular/GPS combo antenna.

This device is configured with default settings and is ready to be configured via HTML. Some configurations may be set using AT commands. Refer to Section XX for AT Commands using the Serial Port.

1.8 RS-232 SERIAL PORT INTEGRATION PARAMETERS

Table 5 provides the serial cable design information to integrate the Vanguard modem into your system. Table 6 gives the default RS-232 communication parameters.

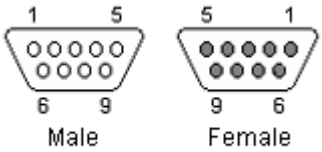
Table 5 – Standard RS-232 DE-9 Pin out

Pin	Name	Direction	Description
1	CD	←	Carrier Detect
2	RX	←	Receive Daa
3	TX	→	Transmit Data
4	DTR	→	Data Terminal Ready
5	GND		System Ground
6	DSR	←	Data Set Ready
7	RTS	→	Request to Send
8	CTS	←	Clear to Send
9	RI	←	Ring Indicator
Note: Direction is DTE relative DCE			

Table 6 – Default RS-232 Communication Parameters

Bits Per Second	115,200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Figure 7 DE-9 Connectors



1.8.1 ODP (OPEN DEVELOPERS PLATFORM) OVER RS-232

This device includes the Open Developers Platform (ODP), which permits customers to develop their own Linux based applications which run on the modem's ARM9 (AT91RM9200) processor. The customer's application can utilize the external RS-232 port, and or an internal 3 pin (GND, RXD, TXD) RS-232 port and is able to transfer data over the cellular WAN using the linux socket libraries. The Vanguard firmware also supports an API that allows the customer's application to access diagnostic data from the cell module such as connection status and RSSI. More information and support is provided by CalAmp's Applications Engineering organization.

2 GETTING STARTED

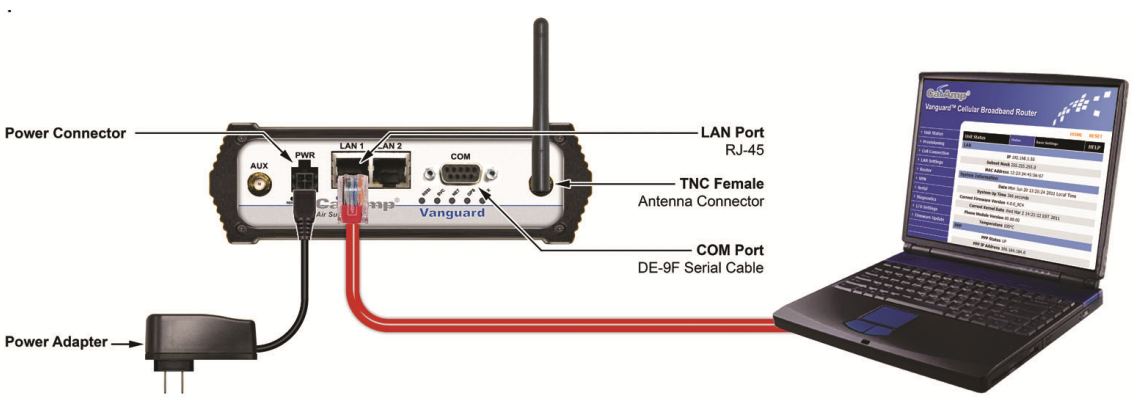
2.1 PACKAGE CONTENTS

- Vanguard Modem
- Power Cable
- Information Card

2.2 DEVICE CONNECTIONS

1. (GSM Users) Insert the SIM card into the SIM/SVC slot as shown.

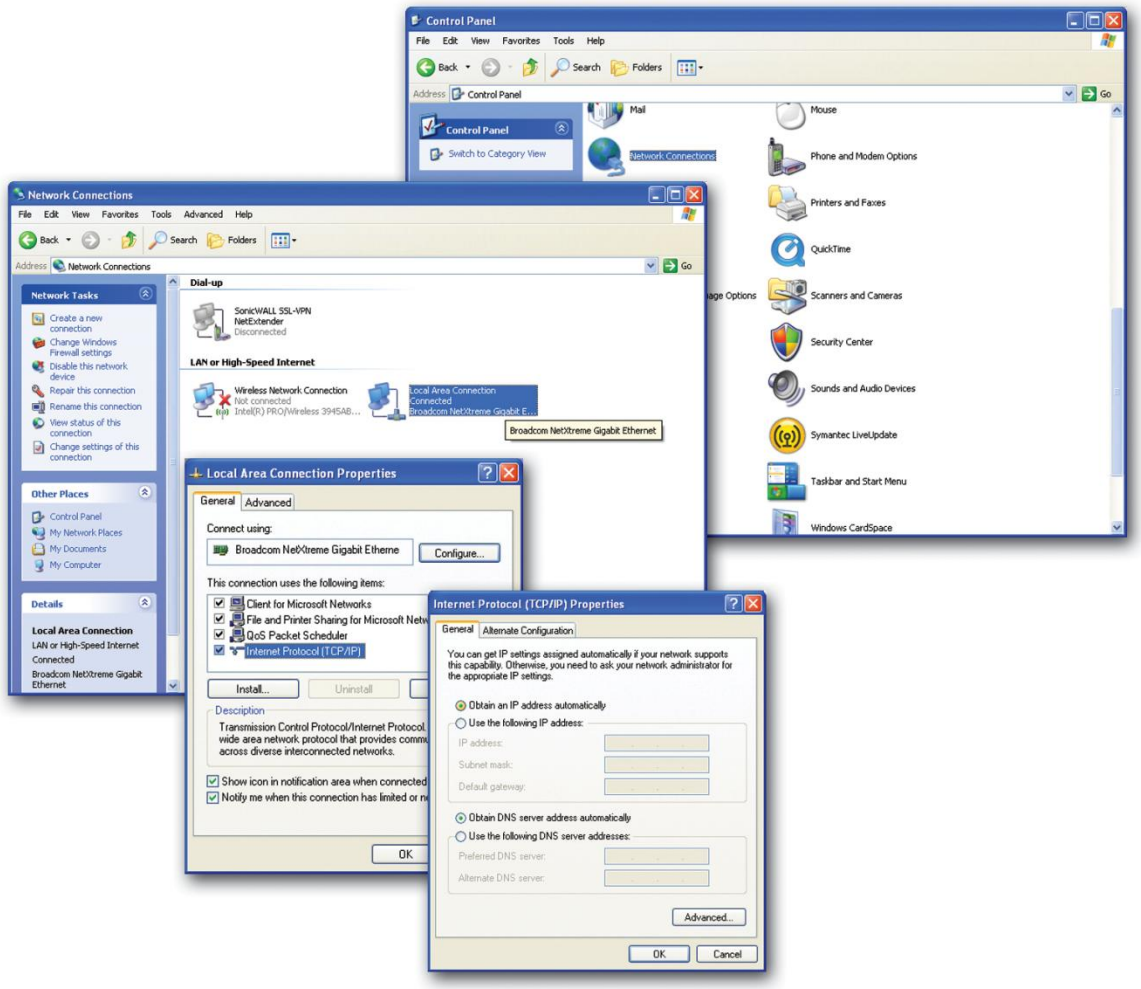
2. Connect an antenna to the ANT connector on the front panel of the Vanguard modem.
3. Connect an Ethernet cable into the LAN 1 port and plug the other end into the network port of your PC.
4. Connect the Power Adapter to the modem PWR port and plug into a proper AC power socket.



2.3 LAN CONFIGURATION

This device is configured via the Internet which automatically allows your computer to obtain the proper IP address. For Windows XP users, select **Start** » **Control Panel** » **Network Connections**. Right click **Local Area Connection** and select **Properties** to open the configuration dialog box for Local Area Connection. Select **Internet Protocol (TCP/IP)** and click **Properties** to open the TCP/IP configuration window. On the General tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to complete TCP/IP configuration.

Figure 8 LAN Configuration Screens



2.4 CELLULAR CONNECTIONS

Before you begin, you will need an active Cellular account with the carrier of your choice.

2.4.1 GSM USERS

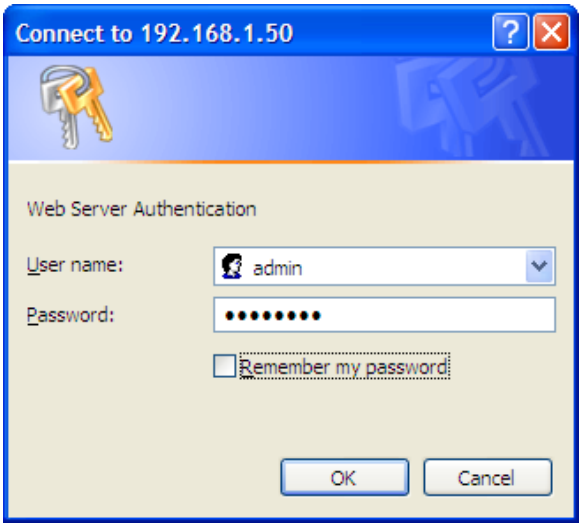
Insert the SIM card with the gold side up into the SIM/SVC slot in the rear of the device. Push the card completely into the slot until it clicks in place. If you have already powered your device, you will need to cycle power to register the SIM for proper operation.

2.4.2 CDMA USERS

Refer to Section 3.3 to provision your modem for proper operation.

3 VANGUARD WEB INTERFACE

Start your web browser and enter 192.168.1.50 in the address bar. A login screen should appear.



Enter the User Name: admin and the Password: password and click OK to log into the modem's Home Page. Vanguard Web interface is divided into two sections. On the left is the main navigation panel (shown in Figures 9-10). On the right is the content area for the desired page (shown in Figures 11-12).

Figure 9 LAN CDMA Main Navigation Panel

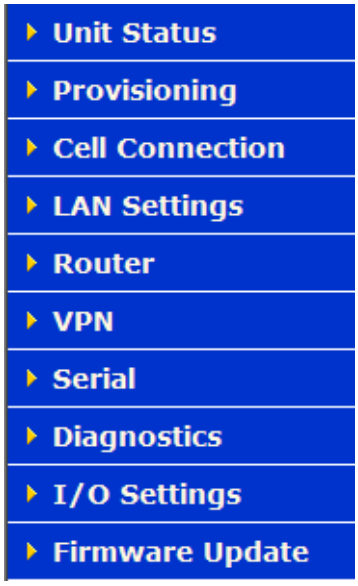
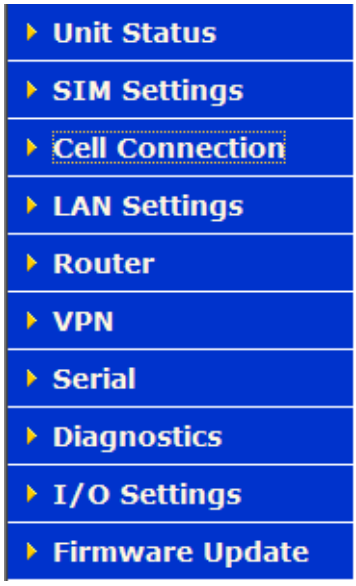


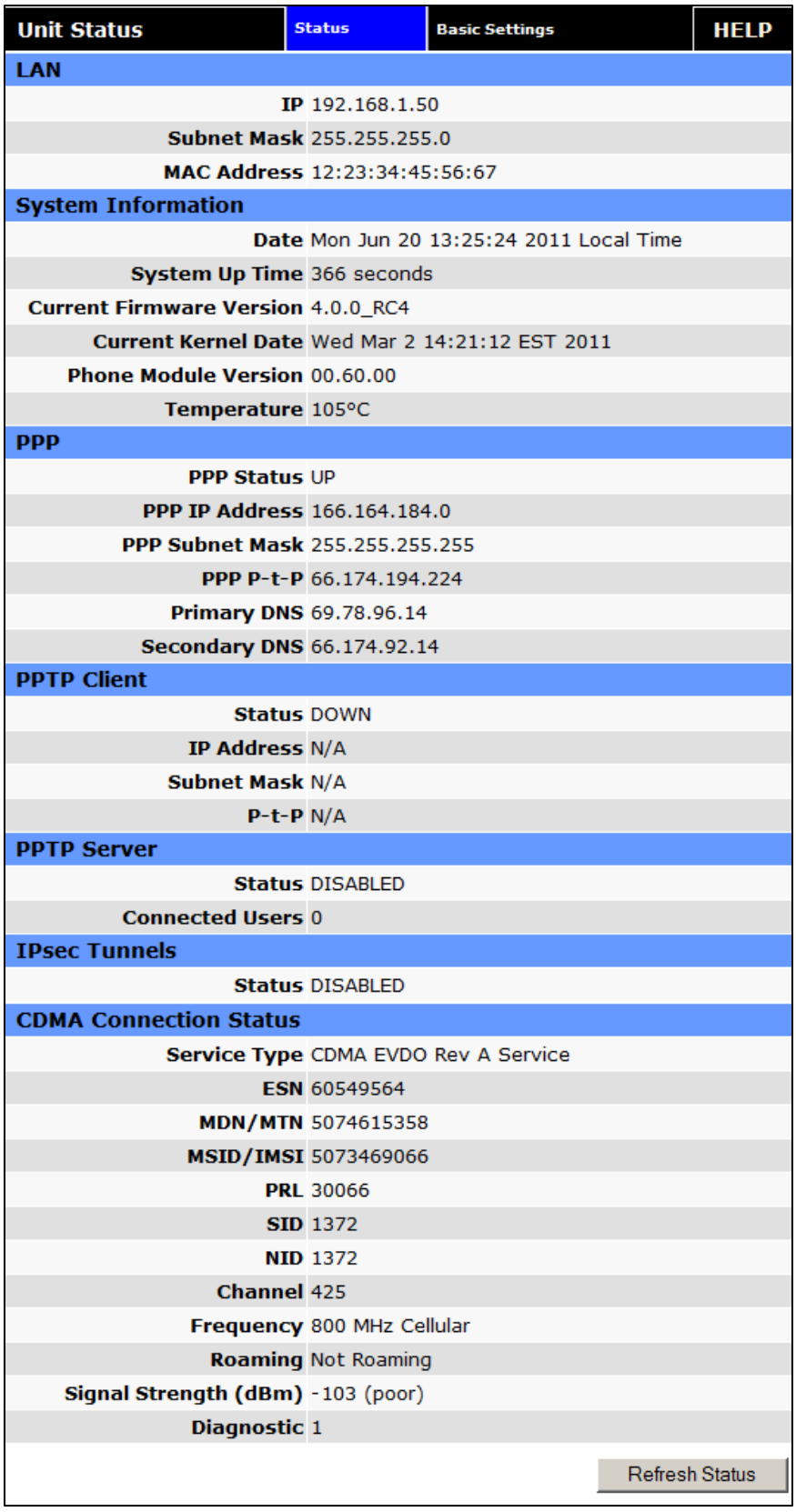
Figure 10 GSM Main Navigation Panel



3.1 UNIT STATUS

3.1.1 STATUS

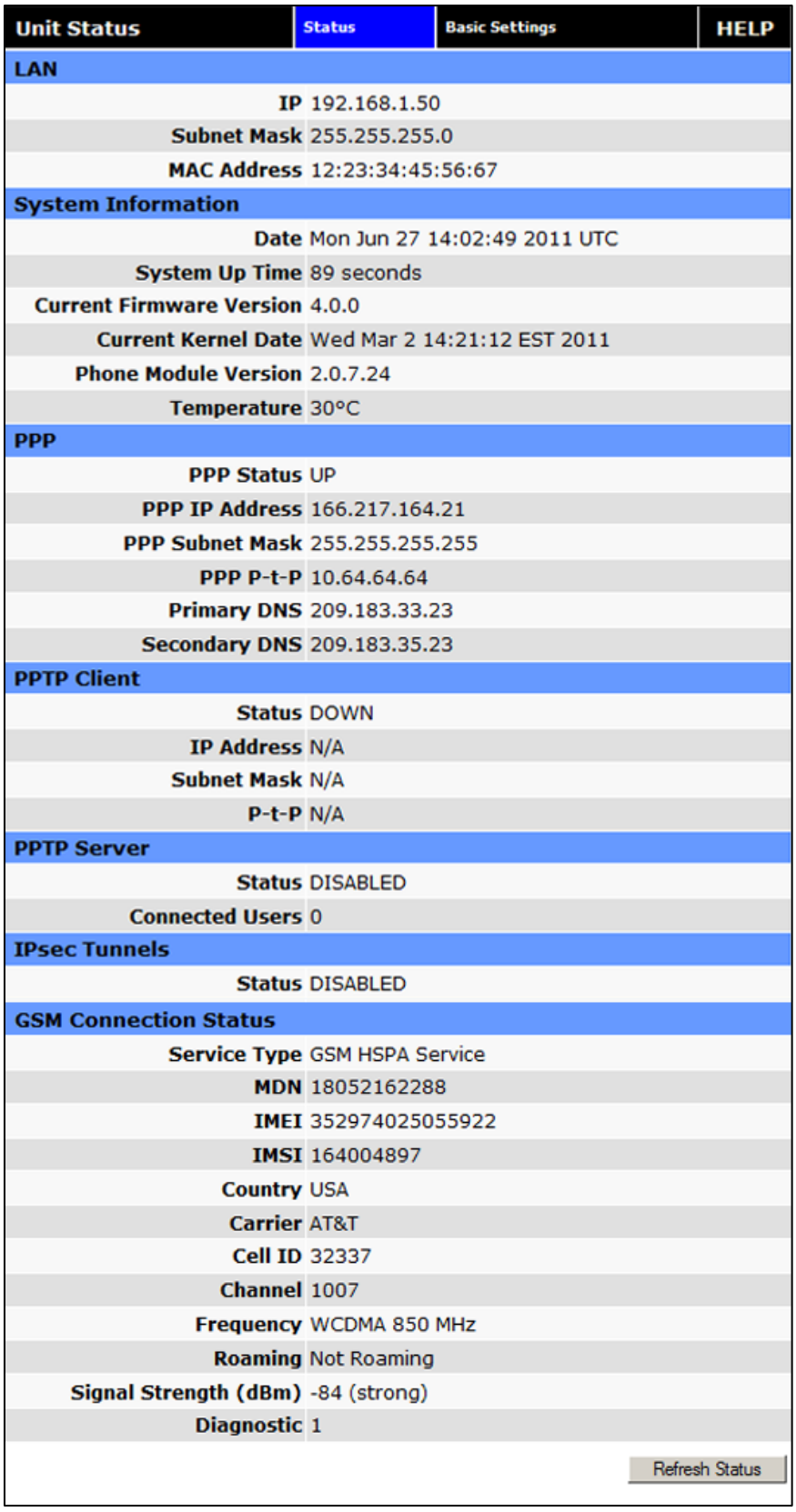
Figure 11: Vanguard CDMA Unit Status Window



Unit Status	Status	Basic Settings	HELP
LAN			
IP	192.168.1.50		
Subnet Mask	255.255.255.0		
MAC Address	12:23:34:45:56:67		
System Information			
Date	Mon Jun 20 13:25:24 2011 Local Time		
System Up Time	366 seconds		
Current Firmware Version	4.0.0_RC4		
Current Kernel Date	Wed Mar 2 14:21:12 EST 2011		
Phone Module Version	00.60.00		
Temperature	105°C		
PPP			
PPP Status	UP		
PPP IP Address	166.164.184.0		
PPP Subnet Mask	255.255.255.255		
PPP P-t-P	66.174.194.224		
Primary DNS	69.78.96.14		
Secondary DNS	66.174.92.14		
PPTP Client			
Status	DOWN		
IP Address	N/A		
Subnet Mask	N/A		
P-t-P	N/A		
PPTP Server			
Status	DISABLED		
Connected Users	0		
IPsec Tunnels			
Status	DISABLED		
CDMA Connection Status			
Service Type	CDMA EVDO Rev A Service		
ESN	60549564		
MDN/MTN	5074615358		
MSID/IMSI	5073469066		
PRL	30066		
SID	1372		
NID	1372		
Channel	425		
Frequency	800 MHz Cellular		
Roaming	Not Roaming		
Signal Strength (dBm)	-103 (poor)		
Diagnostic	1		

Refresh Status

Figure 12: Vanguard GSM Unit Status



Unit Status	Status	Basic Settings	HELP
LAN			
IP	192.168.1.50		
Subnet Mask	255.255.255.0		
MAC Address	12:23:34:45:56:67		
System Information			
Date	Mon Jun 27 14:02:49 2011 UTC		
System Up Time	89 seconds		
Current Firmware Version	4.0.0		
Current Kernel Date	Wed Mar 2 14:21:12 EST 2011		
Phone Module Version	2.0.7.24		
Temperature	30°C		
PPP			
PPP Status	UP		
PPP IP Address	166.217.164.21		
PPP Subnet Mask	255.255.255.255		
PPP P-t-P	10.64.64.64		
Primary DNS	209.183.33.23		
Secondary DNS	209.183.35.23		
PPTP Client			
Status	DOWN		
IP Address	N/A		
Subnet Mask	N/A		
P-t-P	N/A		
PPTP Server			
Status	DISABLED		
Connected Users	0		
IPsec Tunnels			
Status	DISABLED		
GSM Connection Status			
Service Type	GSM HSPA Service		
MDN	18052162288		
IMEI	352974025055922		
IMSI	164004897		
Country	USA		
Carrier	AT&T		
Cell ID	32337		
Channel	1007		
Frequency	WCDMA 850 MHz		
Roaming	Not Roaming		
Signal Strength (dBm)	-84 (strong)		
Diagnostic	1		

Refresh Status

LAN

- **IP**
  Displays LAN side static IP information for this device (the modem). Note: Once this IP address has been changed and saved, the browser connection to the device will be lost. To continue configuration, please connect to the (new) IP address / the address that has been entered and saved.

- **Subnet Mask**
  Displays the LAN side subnet mask for the modem

- **MAC Address**
  Media Access Control Address. Every Ethernet device (i.e. LAN cards) has a unique hardware serial number or MAC address to identify each Network Device from all others.

System Information

- **Date**
  Displays the current date and time (UTC) as received from the cellular carrier. The date and time information is updated at the start of each PPP connection, and then maintained internally until the modem is rebooted. If no PPP connection has been made this boot cycle, the time display will not be accurate. This is not a user settable function – it is controlled only by the carrier supplied date and time. Not all carriers support this function.

- **System Up time**
  Displays the system uptime in seconds:
  - 1 minute = 60 seconds
  - 1 hour = 3600 seconds
  - 1 day = 86400 seconds
  - 1 year = 31,536,000 seconds

- **Current Firmware Version**
  Displays the current modem firmware version loaded. Please visit www.calamp.com for the latest updates.

- **Kernel Date**
  Displays the date of the operating system kernel the unit is running

- **Phone Module Version**
  This will vary depending on the vendor of the radio module inside the modem.

- **Temperature**
  Displays the current internal temperature of the modem, as measured by the cellular radio module

PPP

- **PPP Status**
  Indicates the status of the PPP interface, usually UP when connected properly

- **PPP IP Address**
  Displays the current IP address of the Modem on the cellular network. This address, if public, should be reachable. 10.X.X.X subnets are not routable from the Internet

- **PPP Subnet Mask**
  Usually set to 255.255.255.255, but may be different depending on carrier

- **PPP P-t-P**
  The P-t-P address is your network access point, it may be possible to ping this address to determine if a PPP IP Address assigned is routable from the Internet

- **Primary DNS**
  The Primary DNS server, as assigned by the cellular carrier, when PPP is UP

- **Secondary DNS**
  The Secondary DNS server, as assigned by the cellular carrier, when PPP is UP

PPTP Client

- **PPTP Client Status**
  Indicates the status of the PPTP Client interface, usually UP when connected properly. PPTP is the point-to-Point Tunneling Protocol used to implement a Virtual Private Network (VPN)

- **PPTP IP Address**
  The current IP address assigned to the modem by the VPN server.

- **PPTP Subnet Mask**
  Usually set to 255.255.255.255, but may be different depending on VPN.

- **PPTP P-t-P**
  The PPTP P-t-P is the LAN address of your VPN server.

PPTP Server

- **Status**
  The PPTP Server is either ENABLED or DISABLED based on user's selection on VPN page.

- **Connected Users**
  Number of users currently connected to the PPTP Server

IPsec Tunnels

- **Status**
  The number of established IPsec tunnels based on the number of tunnels Enabled on the VPN | IPsec page.

CDMA Connection Status

- **Service Type**
  Determines the type of network your device has connected to; GPRS, EDGE, UMTS, HSDPA, CDMA 1xRTT, EVDO Rev0 or RevA.

- **ESN**
  The Electronic Serial Number is only applicable for the CDMA product line, carrier specific (Alltel, Verizon, Sprint, etc).

- **MDN/MTN**
  The actual phone number of the device as supplied by the carrier. When the unit is successfully provisioned, the phone number for the user account will be displayed.

- **MIN/IMSI**
  This number is used by the Mobile Telephone Network and will be different if ported from another carrier (not used by end user of device).

- **PRL**
  Preferred Roaming List, only applicable for the CDMA product line, carrier specific (AllTel, Verizon, Sprint, etc).

- **SID**
  System ID (Identity), provided by the Carrier.

- **NID**
  Network Identifier, this is supplied automatically from the network.

- **Channel**
  Cell Site channel number at which the modem is connected and is useful for the carrier in the event of troubleshooting.

- **Frequency**
  Cellular frequency band the modem is using, 800MHz and 1900MHz are mainly in the US and outlying areas. In some cases 900 and 1800 will be seen for European or Foreign carriers.

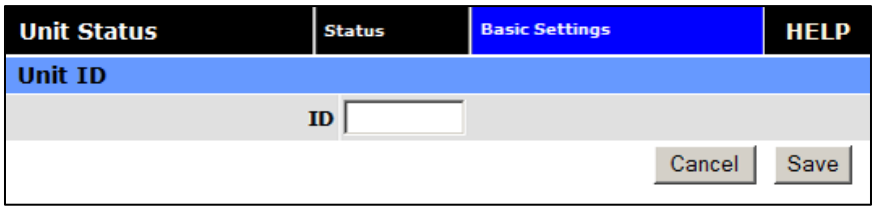
- **Roaming**
  Options are either Roaming or Not Roaming and may defer from the PRL in the case of CDMA.

- **Signal Strength (dBm)**
  Measured in dBm, this is the Received Signal Strength Indicator (RSSI).

- **Diagnostic**
  If less than 128, this is the number of successful PPP connections since the modem was rebooted. If 128 or greater, the formula Diagnostic value – 128 = the number of times the cellular module has been reset since the modem was rebooted.

3.1.2 BASIC SETTINGS

Figure 13: Vanguard CDMA Unit Status – Basic Settings



Unit ID

- **ID**
  This identification number serves to distinguish this unit from other units in the network. It is at the same time the TAIP identification for GPS reporting and serves as the 'syslocation' for the SNMP facility.

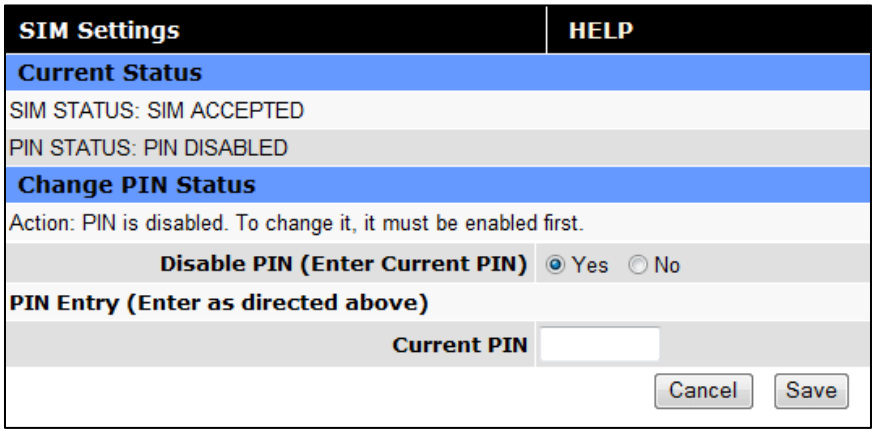
3.2 SIM SETTINGS (GSM MODELS ONLY)

One of the key features of GSM is the Subscriber Identity Module (SIM), commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information. This allows the user to retain his or her information after switching handsets. The SIM has a security feature which, when enabled, will require the user to enter a valid PIN before the modem will connect to the cellular network.

From the Home page, select SIM Settings from the left navigation panel to confirm the modem recognized the SIM card.

SIM STATUS should read ACCEPTED. PIN STATUS may show the PIN to be DISABLED or ACCEPTED. Refer to Section 3 for information on changing the PIN and PIN status.

Figure 14 SIM Settings Page

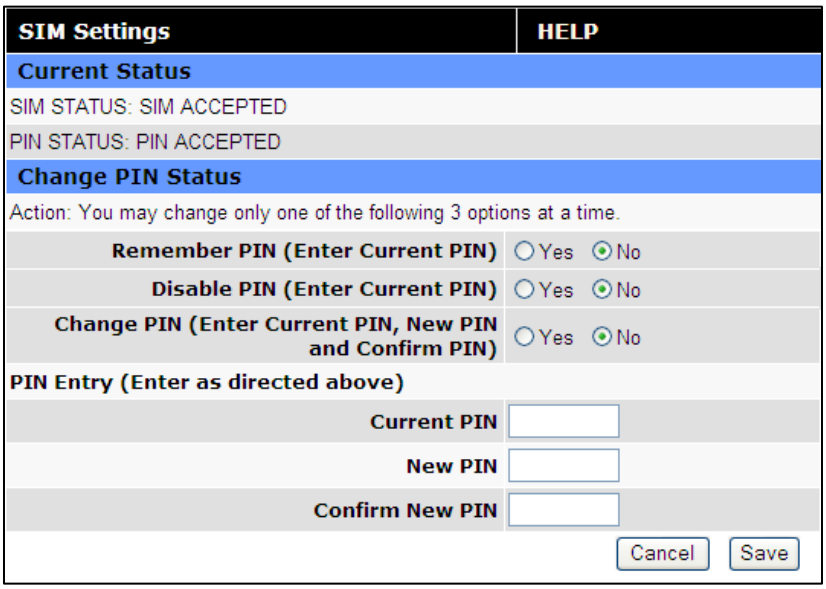


3.2.1 ENABLING PIN SECURITY

As shown in the previous section, the default setting for PIN Security is disabled. Before enabling the PIN Security feature, make sure you have the PIN number provided by your wireless carrier.

Change the Disable PIN setting from Yes (shown in Figure 14) to NO. Enter your carrier provided PIN into the Current PIN field. Click SAVE to access the PIN Security Settings (shown in Figure 15).

Figure 15 PIN ACCEPTED Security Enabled



The PIN security feature is now enabled. PIN STATUS shows that the PIN has been ACCEPTED. Each time modem power is cycled, the proper PIN will need to be entered in order for the modem to dial out. Upon restart, the PIN is entered from the SIM Settings page (shown in Figure 16). The PIN STATUS displays PIN REQUIRED, Enter PIN 3 attempts left.

3.2.2 PIN SECURITY OPTIONS

After PIN security has been enabled, the SIM page will display three options for changing the PIN functionality, **Remember PIN**, **Disable PIN**, or **Change PIN**. Only one of these options can be changed and saved at a time.

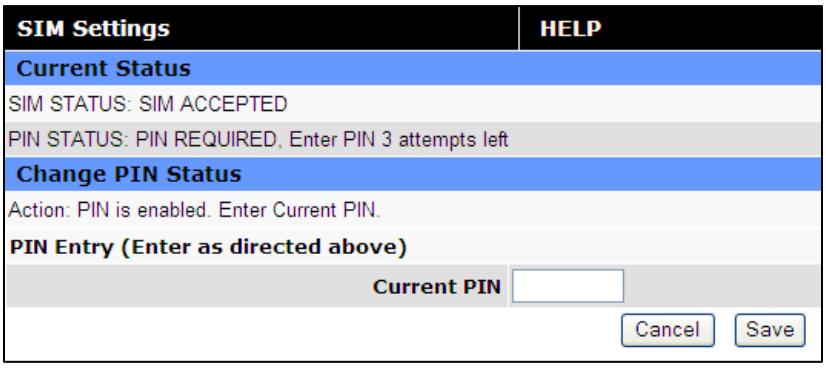
- **Remember PIN:**
  Selecting YES will allow the modem to remember the security PIN making it unnecessary to enter the PIN each time the modem tries to connect to the network. Selecting NO will set the modem to not remember the current PIN, requiring the user to enter the PIN when requested. Since only the modem remembers the PIN, using the SIM card in a different modem will require PIN authorization to dial out.

- **Disable PIN:**
  Selecting YES will disable the PIN security feature; the current PIN will need to be entered to allow disabling. A selection of NO indicates that PIN security is enabled.

- **Change PIN:**
  Selecting YES will allow the user to change the current PIN to a new one. Selecting NO will not require the user to change the PIN in the New PIN and Confirm PIN fields. When changing PINs, the user is required to input the current PIN, the new PIN, and the new PIN again in the fields provided.

After one of the options is changed, click the **SAVE** button to refresh the page showing the changes.

Figure 16 SIM Settings for PIN Required



At this point the user has 3 attempts to enter the correct PIN. If the correct PIN is not entered after 3 attempts, an unlock code or PIN Unblocking Key (PUK) from the service provider will be required before the SIM card is usable again. Figure 17 shows the SIM settings after an incorrect PIN has been entered.

Figure 17 SIM PIN Rejected

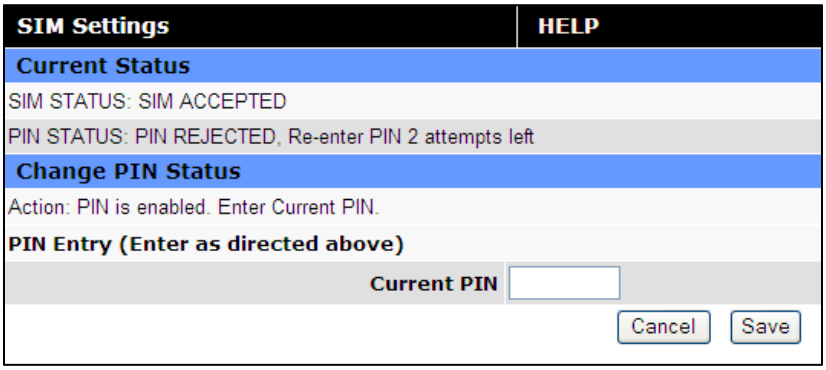
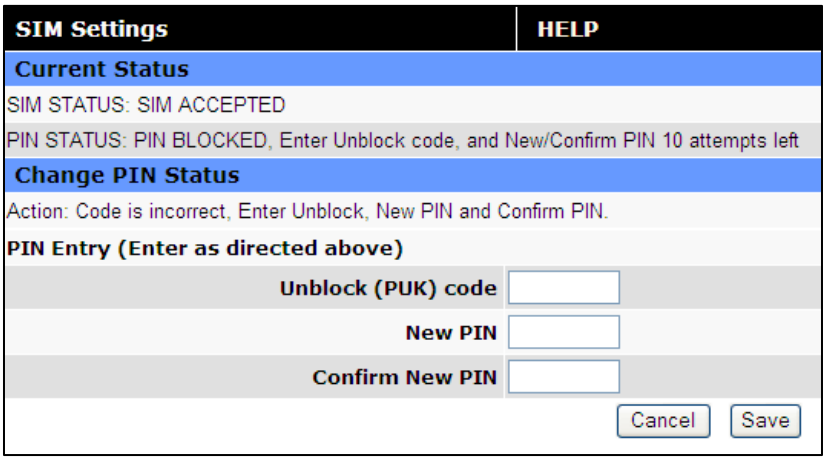


Figure 18 shows the SIM page requiring the unlock code to be entered. At this point the user has 10 attempts to enter the correct unlock code or the SIM card will be rendered unusable.

Figure 18 SIM PIN Unlock – Code Required


SIM Settings
HELP
Current Status
SIM STATUS: SIM ACCEPTED
PIN STATUS: PIN BLOCKED, Enter Unblock code, and New/Confirm PIN 10 attempts left
Change PIN Status
Action: Code is incorrect, Enter Unblock, New PIN and Confirm PIN.
PIN Entry (Enter as directed above)
Unblock (PUK) code
New PIN
Confirm New PIN
Cancel
Save

3.3 PROVISIONING (CDMA MODELS ONLY)

When a CDMA modem is powered up for the first time, most of the provisioning information is blank or has information that needs to be changed. The device is usually shipped with the radio ready to be provisioned on a cellular carrier's network. Features called Over-The-Air Service Provisioning (OTASP) and Internet Over-The-Air (IOTA) are supported, which allow the cellular providers to program the modem with specific information to activate the account.

From the main navigation panel, select provisioning to access the primary provision screen and for access to the advanced settings tab.

3.3.1 VERIZON WIRELESS PROVISIONING INFORMATION (OTASP)

Verizon features Over-The-Air Service Provisioning (OTASP) which allows the cellular provider to provision the modem.

- Provisioning must occur in a non-roaming area of the Verizon network with a medium to strong signal strength.
- Select **Provisioning** from the side menu bar.
- Confirm the OTASP command reads ***22899**.
- Click the **OTASP** button.

If unsuccessful, follow the steps below to enter the information manually. Periodically, you should locally or remotely make sure to click on the OTASP button to ensure the PRL is updated. In some cases this may happen automatically by the carrier.

Manual-Entry Activation

- If provisioning must occur in a roaming area, make sure to have a medium to strong signal strength because manual-entry activation will be required.
- Select **Provisioning** from the side menu bar.
- Input the MDN/MTN and MSID/IMSI (MIN) given by your provider
- Put 6 0's (000000) for the unlock code
- Click the **Write MDN/MSID** button.

3.3.2 SPRINT PROVISIONING INFORMATION (OMA-DM)

Sprint features Open Mobile Alliance Device Management (OMA-DM) which allows the cellular provider to provision the modem.

After the account is activated by Sprint, the device will auto-provision after power is applied to the device for the first time. First, verify on the Home page the MDN/MTN and MSID/IMSI/MIN are in the default mode. Then after 3-4 minutes, check again that the MDN/MTN and MSID/IMSI/MIN are populated with the numbers provided by the carrier. Once this is complete, you can move on to the next section. If auto-provisioning doesn't occur, push the OMA-DM button to provision. If both of these are unsuccessful, follow the steps below to deactivate auto-provisioning and enter the information manually.

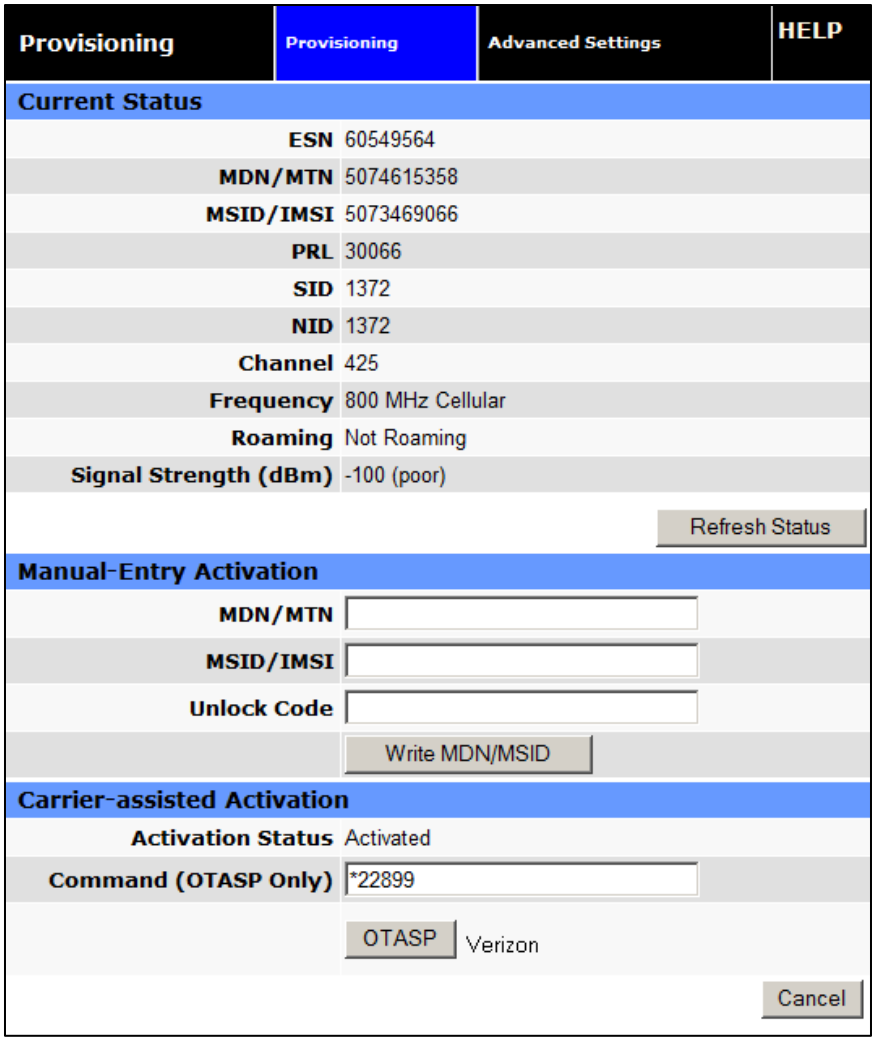
- **Provisioning must occur in a non-roaming area of the Sprint network with a medium to strong** signal strength.
- Select **Provisioning** from the side menu bar.
- Sprint is capable of automatic OMA-DM provisioning. The Auto Activation can be Enabled or Disabled. To save the Auto Activation, click the SAVE button.
- If Auto Activation is Disabled, a manual initiation of OMA-DM can be started by clicking on the OMA-DM button

- If the auto-provisioning fails, and OMA-DM manual provisioning fails, and your outside the Sprint network, follow the manual-entry activation steps below.

Manual-Entry Activation

- If provisioning must occur in a roaming area, make sure to have a medium to strong signal strength because manual-entry activation will be required.
- Select **Provisioning** from the side menu bar.
- Input the MDN/MTN and MSID/IMSI (MIN) given by your provider.
- Put in the unlock code given by your provider.
- Click the **Write MDN/MSID** button.

Figure 19: Vanguard CDMA Provisioning Window



Current Status

- **ESN**

The Electronic Serial Number is only applicable for the CDMA product line, carrier specific (Alltel, Verizon, Sprint, etc). This number is used to set up the user account with the cellular provider.

- **MDN/MTN**
  The actual phone number of the device as supplied by the carrier. When the unit is successfully provisioned, the phone number for the user account will be displayed.

- **MIN/IMSI**
  This number is used by the Mobile Telephone Network and will be different if ported from another carrier (not used by end user of device).

- **PRL**
  Preferred Roaming List, only applicable for the CDMA product line, carrier specific (Alltel, Verizon, Sprint, etc).

- **SID**
  System ID (Identity), provided by the Carrier.

- **NID**
  Network Identifier, this is supplied automatically from the network.

- **Channel**
  Cell Site channel number to which the modem is connected. This number can be useful to the cellular provider for troubleshooting purposes.

- **Frequency**
  Cellular frequency band the modem is using, 800MHz and 1900MHz are mainly in the US and outlying areas. In some cases 900 and 1800 will be seen for European or Foreign carriers.

- **Roaming**
  Options are either Roaming or Not Roaming and may defer from the PRL in the case of CDMA. For provisioning, the unit must NOT be roaming.

- **Signal Strength (dBm)**
  Measured in dBm, this is the Received Signal Strength Indicator (RSSI). For provisioning, the signal strength should be greater than -95 dBm.

Manual-Entry Activation

- **MDN/MTN**
  The Mobile Directory Number assigned by the cellular provider for the specific ESN on the user account.

- **MSID/IMSI**
  MSID, which only needs to be entered if different than the MDN.

- **Unlock Code**
  A carrier supplied activation code (usually 6 or 7 digits for Sprint accounts).

Click the Write MDN/MSID button when the required information has been entered.

Enable/Disable OMA-DM Activation

This section will only be displayed for units which are capable of automatic (OMA-DM) provisioning. You may choose to enable or disable the automatic provisioning and save your desired setting. If enabled, and the unit is not provisioned (activated), each time at power-on (only) the unit will attempt an auto-activation. This capability is dependent on whether or not it is offered by your cellular carrier.

- **Auto-Activation**
  Choose Enable to direct an unprovisioned unit to attempt OMA-DM activation once per power-up.

Click **SAVE** to activate the desired settings.

Manual Initiation of OMA-DM Provisioning

This section will only be displayed for units which are capable of automatic (OMA-DM) provisioning. The activation status is displayed, and a button is provided to direct the unit to begin an OMA-DM provisioning attempt. Depending on changes to your carrier's network, it may be necessary to re-provision a unit that has already been activated. The OMA-DM capability is dependant on whether or not it is offered by your cellular carrier.

- Activation Status
  Displays the device activation status: Activated or Not Activated

Click **OMA-DM** to trigger an OMA-DM provisioning attempt.

Activation Type

This section is displayed for units that are not capable of automatic (OMA-DM) provisioning. Availability of OMA-DM is carrier dependant. For carriers that do not support OMA-DM, the provisioning process must be triggered by entering carrier specific information and depressing the carrier specified button (OTASP or IOTA).

- Command (OTASP Only)
  The dial command used for provisioning the modem. For OTASP the number is *22899. For IOTA this field is left blank.

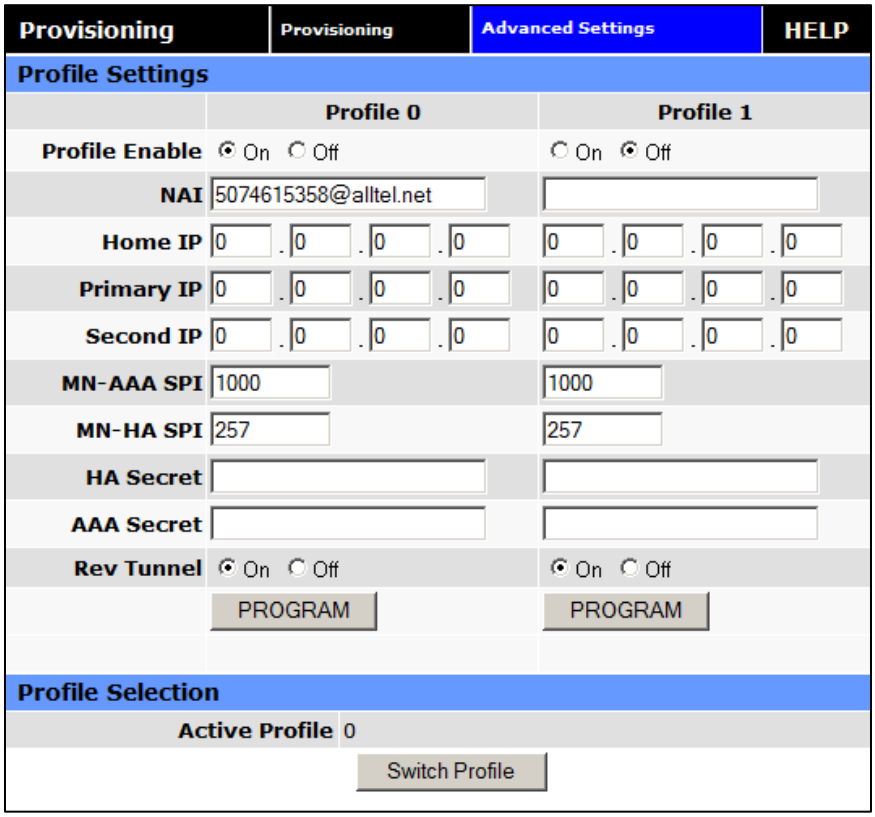
Click **OTASP** button to start the provisioning process for units using Verizon.

Click the **IOTA** button to start the provisioning process for units using Sprint.

3.3.3 ADVANCED SETTINGS

The Advanced Settings screen supports the programming of 2 profiles that may be used to login to the cellular provider's network. It also allows the user to choose which profile is active. A provider may support alternate networks whose use is limited to specific customers. Login information must be gathered from the provider. Be aware that incorrect parameter settings could result in no access to the standard network, and no access to the alternate network.

Figure 20: Vanguard CDMA Provisioning – Advanced Settings



Profile Settings

- **Profile Enable**
  This field indicates if the profile is enabled. It is possible to enable both profiles. Whether to enable 1 or both profiles should be based on information from the provider

- **NAI**
  Network Address ID. This field should be set the NAI supplied by the provider.

- **Home IP Address**
  This parameter should be set to the Home IP Address supplied by the provider.

- **Primary IP Address**
  This parameter should be set to the Primary Home Agent IP Address supplied by the provider.

- **Second IP Address**
  This parameter should be set to the Secondary Home Agent IP Address supplied by the provider.

- **MN-AAA SPI**
  This parameter should be set to the MN-AAA SPI setting supplied by the provider. This is a numeric setting.

- **MN-HA SPI**
  This parameter should be set to the MN-HA SPI setting supplied by the provider. This is a numeric setting.

- **HA Secret**
  This parameter should be set to the Home Agent Secret (password) supplied by the provider.

- **AAA Secret**
  This parameter should be set to the AAA Shared Secret (password) supplied by the provider.

- **Rev Tunnel**
  Reverse Tunneling may be enabled or disabled, as specified by the provider.

- **Program**
  Pressing the program button will prompt you to confirm you wish to program the current displayed settings. If confirmed, the settings will be programmed and the unit will reboot.

Profile Selection

- **Active Profile**
  Displays which profile is active. The field cannot be modified, instead press the Change button to select the other profile.

- **Switch Profile**
  Pressing the Switch Profile button will prompt you to confirm you wish to switch to activate the other profile. If confirmed, the other profile will be selected and the unit will reboot.

3.4 CELL CONNECTION

Select **Cell Connection** from the main navigation pane for user access to the Dial Settings, System Monitor and Dynamic DNS configuration screens.

3.4.1 DIAL SETTINGS

The Dial Settings screen configures the dialing properties to initiate a data call with the cellular provider.

Figure 21: Vanguard CDMA Cell Connection – Dial Settings

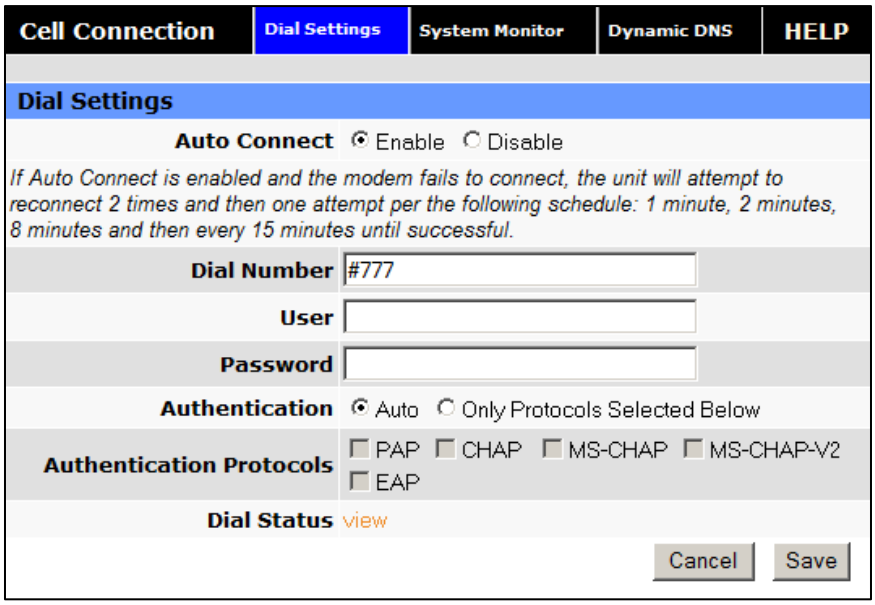
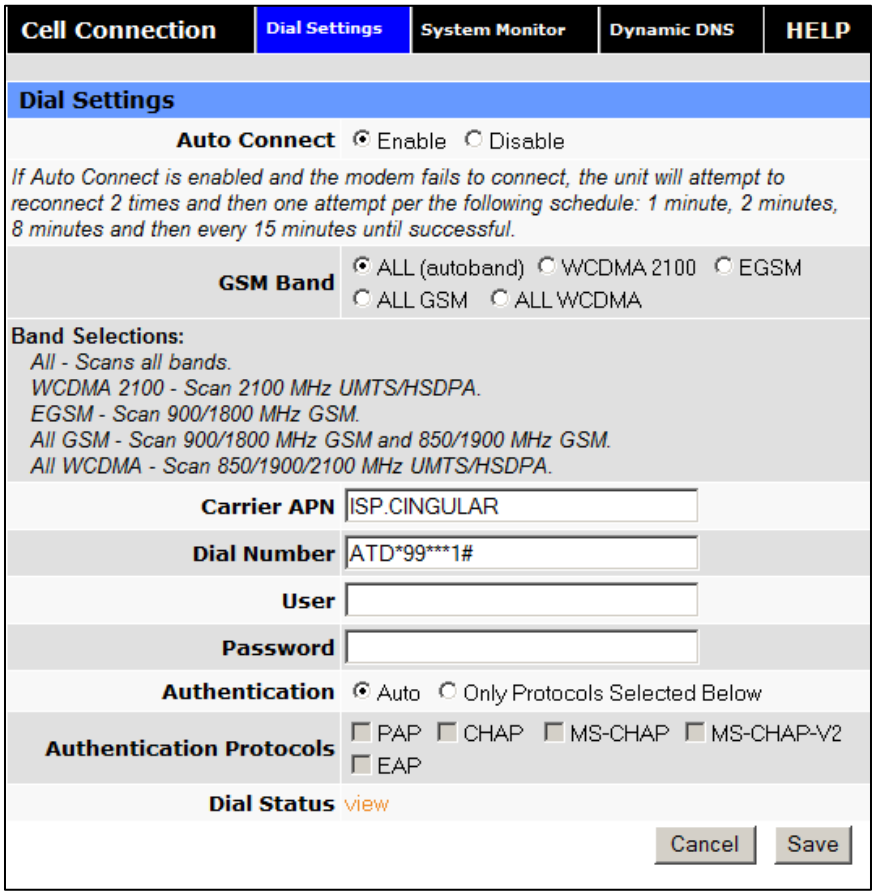


Figure 22: Vanguard GSM Cell Connection – Dial Settings



Dial Settings

- **Auto Connect**
  When set to Enable, will allow the modem to automatically dial the connection when the modem is powered. When set to Disable, the modem will not automatically dial the connection to the cellular provider and will not attempt to automatically re-connect when the connection has dropped.

- **Dial Number**
  The phone number used to initiate a data connection to the cellular provider via PPP. The default dial number is #777.

- **User**
  Sets the username required by the cellular provider. Leave blank if not required. Warning: If used in combination with this modem's VPN Server, this username and password will also be valid on this modem's VPN Server.

- **Password**
  Sets the password required by the cellular provider. Leave blank if not required.Warning: If used in combination with this modem's VPN Server, this username and password will also be valid on this modem's VPN Server.

- **Authentication**
  Select the authentication protocol used. If **Auto** is selected, the Vanguard will automatically select a protocol. If **Only Protocols Selected Below** is chosen, the router will only accept requests for the specified protocols.

- **Authentication Protocols**
  If Only Protocols Selected Below is chosen, then these fields are used to specify each Authentication protocol that router will accept. At least 1 must be selected. If Auto is selected, these choices will be disabled (greyed out).

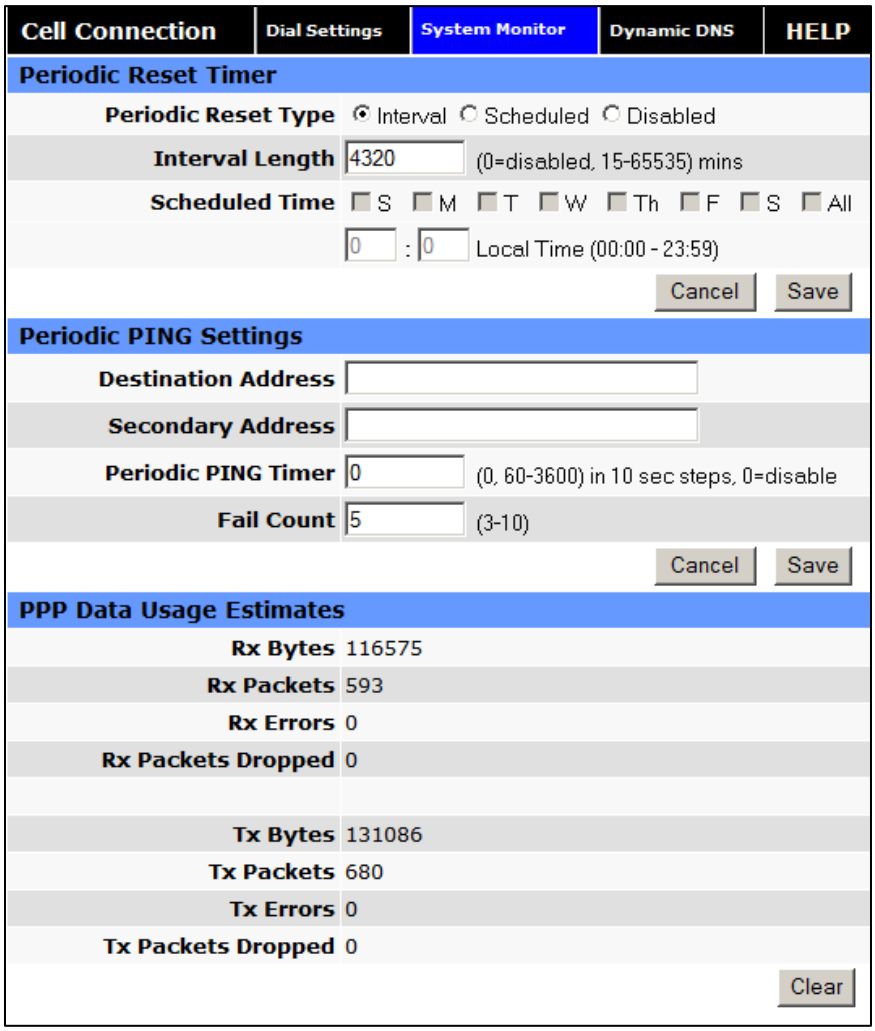
- **Dial Status**
  Click “View” to see a log from the last connection attempt.

The **SAVE** button must be pressed for changes to take effect.

3.4.2 SYSTEM MONITOR

Select **Cell Connection** from the left navigation pane. The System Monitor tab allows user access to the configuration of additional self-monitoring for the modem to determine when service provider connections may have been terminated.

Figure 23: Vanguard Cell Connection – System Monitor



Periodic Reset Timer

- **Periodic Reset Type**
  Sets the Periodic Modem Reset timer to an Interval time, a Scheduled day, or disables it.

- **Interval Length**
  Sets the Periodic Modem Reset time from 15 to 65,535 minutes. The Periodic Reset is disabled when set to 0. Default is set to 4320 min. (approximately 3 days)

- **Scheduled Time**
  Sets the Periodic Modem Reset to occur at the specified time. Select the days of week desired or 'All' for everyday. Time is specified as Local Time, based on the location of the modem itself. The modem's current time is shown on the "home" page.

Periodic Ping Settings

- **Destination Address**
  User may enter an accessible IP address or URL that will respond to a ping command.

- **Secondary Address**
  User may enter an accessible IP address or URL that will respond to a ping command. This address will be used if the entered number of consecutive ping failures using the first address is reached.

- **Periodic Ping Timer**
  User may enter an interval in increments of 10 seconds. The modem will ping the destination at that interval. Enter 0 to disable this feature.

- **Fail Count**
  The modem will reset if the number of consecutive ping failures is equal to or greater than this entry and the secondary address is being used. Otherwise the modem will switch from the first address to the secondary address for the ping test.

PPP Data Usage Estimates

This section tracks the data received from and transmitted to the cellular network. This is a tool that may be used to estimate network usage. These totals are tracked by the router. Your carrier maintains separate statistics from which your billing is determined. One way to use this tool is to track usage over a fairly short period of typical usage. The total then can be extrapolated to estimate longer time periods. This router updates these statistics once approximately every 30 seconds. Press the Clear button to reset the totals to 0.

- **Rx Bytes**
  The total number of bytes received by the modem from the cell network. All statistics will be cleared automatically if this count exceeds 1 billion (1,000,000,000).

- **Rx Packets**
  The total number of TCP and UDP packets received by the modem from the cell network.

- **Rx Errors**
  The number of corrupted TCP and UDP packets received by the modem from the cell network.

- **Rx Packets Dropped**
  The number of TCP and UDP packets received by the modem from the cell network that were not accepted. This may occur due to memory or throughput problems.

- **Tx Bytes**
  The total number of bytes transmitted by the modem to the cell network. All statistics will be cleared automatically if this count exceeds 1 billion (1,000,000,000).

- **Tx Packets**
  The total number of TCP and UDP packets transmitted by the modem to the cell network.

- **Tx Errors**

The number of corrupted TCP and UDP packets received by the modem that were meant to be transmitted on the cell network.

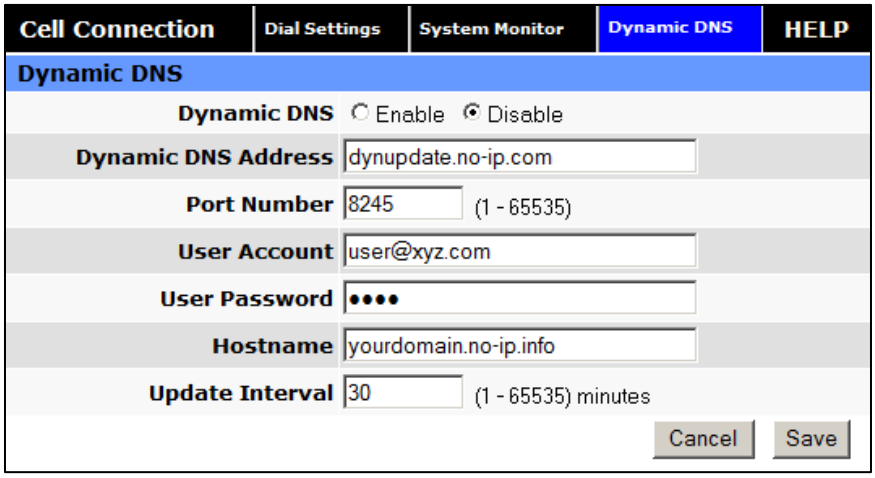
- **Tx Packets Dropped**
  The number of TCP and UDP packets received by the modem for transmit to the cell network that were not accepted. This may occur due to memory or throughput problems.

Press **Clear** to reset the totals to 0. These totals are NOT cleared by a modem reboot.

3.4.3 DYNAMIC DNS

Select **Cell Connections** from the left navigation pane. Select the Dynamic DNS tab to open the Dynamic DNS configuration page. Dynamic DNS is a system which allows the domain name data of a computer with a varying (dynamic) IP addresses held in a name server to be updated in real time in order to make it possible to establish connections to that machine without the need to track the actual IP address themselves at all times. A number of providers offer Dynamic DNS services ("DDNS"), free or for a charge. For example, a free service provided by NO-IP allows users to setup between one and five host names on a domain name provided by NO-IP. No-IP is the default DNS service.

Figure 24: Vanguard Cell Connection – Dynamic DNS



Dynamic DNS

- **Dynamic DNS**
  Selecting Enable will allow the modem to provide the selected service dynamic IP address information. Selecting Disable will stop any IP information from being sent to the selected service.

- **Dynamic DNS Address**
  The internet address to communicate the Dynamic DNS information to. Default is dynupdate.no-ip.com.

- **Port Number**
  The port number for the internet address give above. Default is 8245.

- **User Account**

The username used when setting up the account. Used to login to the Dynamic DNS service.

- **User Password**
  The password associated with the username account.

- **Hostname**
  The hostname identified to the Dynamic DNS service. For example http:/test.myserver.com.

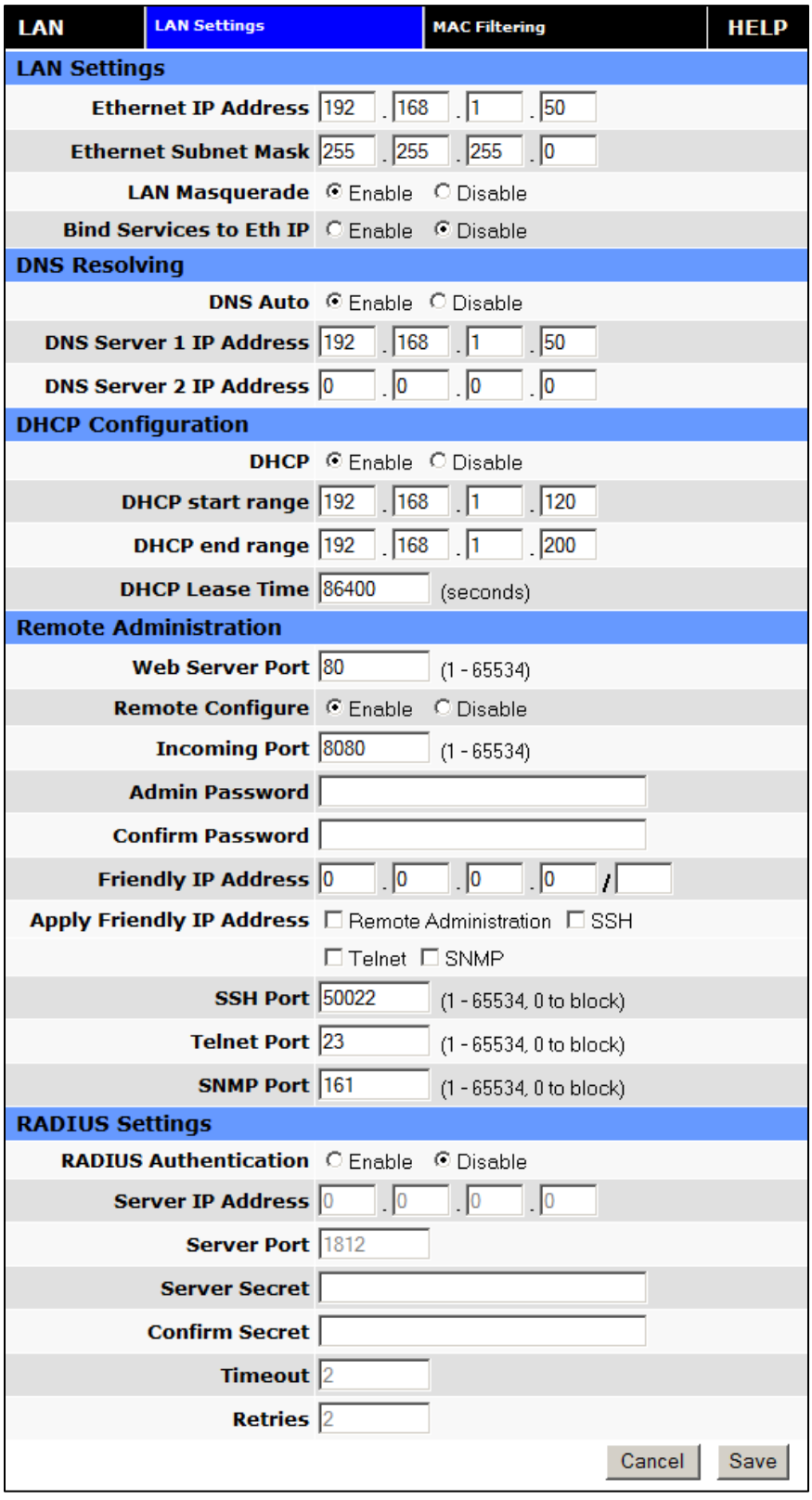
- **Update Interval**
  Sets the interval, in minutes (0 to 65,535), the modem will update the Dynamic DNS server of its carrier assigned IP address. It is recommended to set this interval as long as necessary. Each update is considered a data call by the cellular provider and could deplete low usage data plan minutes.

The **SAVE** button must be pressed for changes to take effect.

3.5 LAN SETTINGS

Select **LAN Settings** from the main navigation pane for access to LAN configuration settings and the MAC Filtering tab.

Figure 25: Vanguard LAN Settings Window


LAN
LAN Settings
MAC Filtering
HELP
LAN Settings
Ethernet IP Address 192 . 168 . 1 . 50
Ethernet Subnet Mask 255 . 255 . 255 . 0
LAN Masquerade Enable Disable
Bind Services to Eth IP Enable Disable
DNS Resolving
DNS Auto Enable Disable
DNS Server 1 IP Address 192 . 168 . 1 . 50
DNS Server 2 IP Address 0 . 0 . 0 . 0
DHCP Configuration
DHCP Enable Disable
DHCP start range 192 . 168 . 1 . 120
DHCP end range 192 . 168 . 1 . 200
DHCP Lease Time 86400 (seconds)
Remote Administration
Web Server Port 80 (1 - 65534)
Remote Configure Enable Disable
Incoming Port 8080 (1 - 65534)
Admin Password
Confirm Password
Friendly IP Address 0 . 0 . 0 . 0 /
Apply Friendly IP Address Remote Administration SSH
Telnet SNMP
SSH Port 50022 (1 - 65534, 0 to block)
Telnet Port 23 (1 - 65534, 0 to block)
SNMP Port 161 (1 - 65534, 0 to block)
RADIUS Settings
RADIUS Authentication Enable Disable
Server IP Address 0 . 0 . 0 . 0
Server Port 1812
Server Secret
Confirm Secret
Timeout 2
Retries 2
Cancel
Save

LAN Settings

- **Ethernet IP Address**
  This sets the IP address of this device and is the address used to access the configuration pages. If the IP address changes you will have to re-enter the new IP address in your browser to access the configuration pages. The default IP is 192.168.1.50 and should be changed for security purposes.

- **Ethernet Subnet Mask**
  Sets the subnet mask for the LAN side of the modem to the device

- **LAN Masquerade**
  When enabled the Vanguard masquerades all Ethernet traffic to the LAN, making all WAN traffic appear as if it originated from the Vanguard. This can be useful in applications where less-capable equipment on the local LAN cannot cope with connections from multiple Host IP addresses

- **Bind Services to Eth IP**
  UDP datagrams or TCP sockets from services inside the Vanguard (Serial, IO, GPS) normally appear to come from the interface (LAN or WAN) closest to the destination. Enable this option to force the source address to be the LAN Ethernet IP address. This can be useful if packets are being sent through a VPN tunnel. Note that outside of a tunnel, NAT may still force the source address to be rewritten to the WAN address.

DNS Resolving

- **DNS Auto**
  Selecting Enable will allow the servers set as DNS Server 1 or 2 to automatically resolve domain names to IP addresses. These servers communicate with name servers by sending DNS queries and heeding DNS responses. Selecting Disable will not allow DNS Sever 1 or 2 to resolve domain names.

- **DNS Server 1 IP Address**
  The Ethernet IP address of the preferred DNS server. The default address is 192.168.1.50, the same as the LAN Ethernet IP Address for the modem. If the LAN Ethernet ID Address changes, the DNS Server 1 address will automatically change to the same.

- **DNS Server 2 IP Address**
  Ethernet address of the alternate DNS server. The default is set to 0.0.0.0.

DHCP Configuration

- **DHCP**
  Dynamic Host Configuration Protocol; a protocol used by client devices that are connected to the LAN port of this device to automatically obtain an IP address assigned by this device. Selecting Enable will configure this device to assign IP addresses to client devices taken from a pool specified by the values entered in DHCP start range and DHCP end range. Selecting Disable will turn off this DHCP server functionality

- **DHCP start range**
  DHCP server starting IP address. The default is set as 192.168.1.100

- **DHCP end range**
  DHCP server ending IP address. The maximum usable number is 253

- **DHCP Lease Time**
  Sets the duration, in seconds, the connected device is allowed to keep the assigned IP address. In many cases it is possible for the device to receive the same IP address after the lease time expires.

Remote Administration

- **Web Server Port**
  Enter the port number to be used by the web server

- **Remote Configure**
  Selecting Enable will allow remote access to the modem's configuration screens through the cellular network connection. Selecting Disable will shut off the ability to remotely access the modem's configuration screens

- **Incoming Port**
  Sets the port number used to remotely configure the modem. (Note: Remote Configuration will be unavailable if the Incoming Port number also appears in an entry in Router | Port Forwarding | IP Mapping Table.)

- **Admin Password**
  Sets the password required for remote configuration

- **Confirm Password**
  Re-type the Admin Password to confirm the correct spelling

- **Friendly IP Address**
  Specifies the IP address from which remote administration is permitted. Entering 0.0.0.0 will allow any IP address. Leave the fifth box blank (after the /) if specifying a specific IP, or 0.0.0.0. A subnet mask may be entered in the fifth box. The mask indicates how many bits of the IP address to match. This can be a value from 1 to 32.

- **Apply Friendly IP Address**
  Check the box next to a service to allow remote access to the service only from the friendly IP address. Uncheck this box to allow any IP address access.

- **SSH, Telnet, and SNMP Ports**
  Enter the port number that will be used for remote access to the service. Entering zero for the port number will block remote access to the service. Once a service is blocked (0 entered) or moved to another port, the default port number (such as 23 for Telnet) can be used in a Port Forwarding rule to provide access to a user device located behind the modem. Port Forwarding has precedence so if the SSH, Telnet or SNMP port also appears as an Incoming Port in an entry in Router | Port Forwarding | IP Mapping Table then that service will be unavailable.

RADIUS Settings

- **RADIUS Authentication**

Enable or disable RADIUS authentication for webpage access

- **Server IP Address**
  The IP address of the RADIUS server

- **Server Port**
  The port of the server

- **Server Secret**
  Sets the secret to use with the server

- **Confim Secret**
  Re-type the Server Secret to confirm the correct spelling

- **Timeout**
  Specify how many seconds to wait before a retry

- **Retries**
  Specify how many times to retry authenticating with the server before giving up

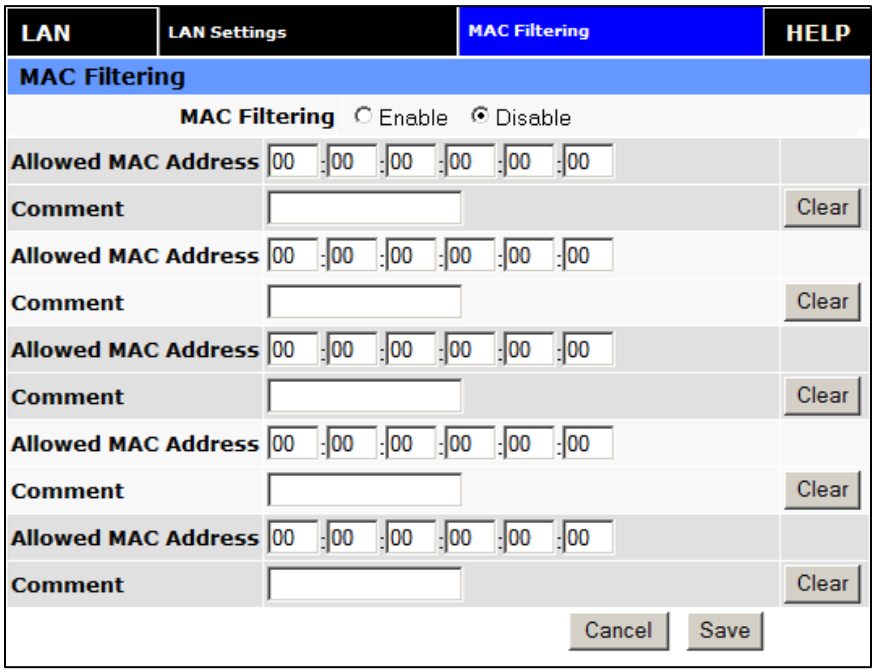
Press **Save** to keep the currently displayed value for each parameter. Once Save is pressed, Cancel cannot be used to return to previous settings.

Press **Cancel** to abort changes and redisplay the last saved parameters for this page.

3.5.1 MAC FILTERING

Select **LAN Settings** from the left navigation pane. The MAC Filtering tab opens the MAC filtering configuration page. MAC filtering allows up to five unique device MAC addresses access to the network.

Figure 26: Vanguard LAN Settings – MAC Filtering



MAC Filtering

- **MAC Filtering**
  Radio button selection to Enable/Disable MAC filtering

- **Allowed MAC Address**
  Enter the MAC address for a device to be allowed on the network.

- **Comment**
  Here a name can be inserted describing the device using the allowed MAC address.

- **Clear**
  Press to remove the MAC address from the list of allowed addresses.

Press **SAVE/CANCEL** to implement or cancel changes.

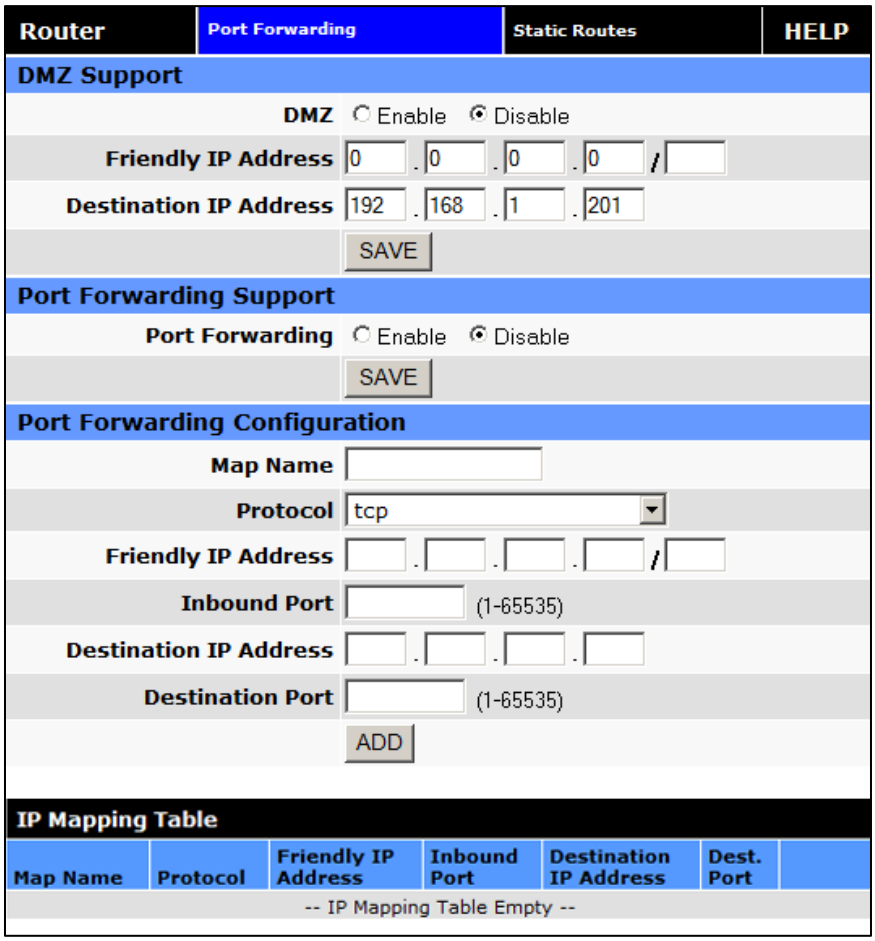
3.6 ROUTER

Select **Router** from the left navigation pane for user access to Port Forwarding and Static Routing tabs.

3.6.1 PORT FORWARDING

Port Forwarding is a technique for transmitting and receiving network traffic through a router that involves re-writing the source and/or destination IP addresses and usually the TCP/UDP port numbers of IP packets as they pass through. The various routing configurations will be displayed in the IP mapping table at the bottom of the screen.

Figure 27: Vanguard Router – Port Forwarding



DMZ Support

DMZ is a host on the internal network that has all ports exposed, except those ports forwarded otherwise.

- **DMZ**
  Radio button selection to Enable/Disable; Select Enable to allow the modem to use DMZ routes using the address set in the Destination IP Address. Select Disable to shut down the DMZ functionality.

- **Friendly IP Address**
  Optionally restricts DMZ access to only the specified IP address. If set to "0.0.0.0", the DMZ is open to all incoming IP Addresses.

- **Destination IP Address**
  The IP address which has all ports exposed, except ports defined in the Port Forwarding configuration.

The **SAVE** button must be pressed for changes to take effect.

Port Forwarding Support

- **Port Forwarding**
  Radio button selection to Enable/Disable. Select Enable to allow the modem to use the Port Forwarding routes described in the IP mapping table. Select Disable to shut down the Port Forwarding functionality.

The **SAVE** button must be pressed for changes to take effect.

Port Forwarding Configuration

- **Map Name**
  Sets the Map Name for the IP mapping table at the bottom of the screen. The Map Name can be up to ten characters in length. Do not use spaces in the character string

- **Protocol**
  Sets the data protocol as either tcp, udp, or all

- **Friendly IP Address**
  Specifies an IP address that is allowed to access the modem or a wildcard IP address of 0.0.0.0 that allows all IP addresses to access the modem. Leave the fifth box blank (after the /) if specifying a specific IP, or 0.0.0.0. A subnet mask may be entered in the fifth box. The mask indicates how many bits of the IP address to match. This can be a value from 1 to 32.

- **Inbound Port**
  Sets the external port number for incoming requests. (Note: Port Forwarding rules take precedence over the services specified in LAN Settings | Remote Administration | Incoming port, SSH Port, Telnet Port or SNMP Port.)

- **Destination IP Address**
  Sets the Local Area Network Address of the device connected to the modem's Ethernet jack. Inbound requests will be forwarded to this IP address.

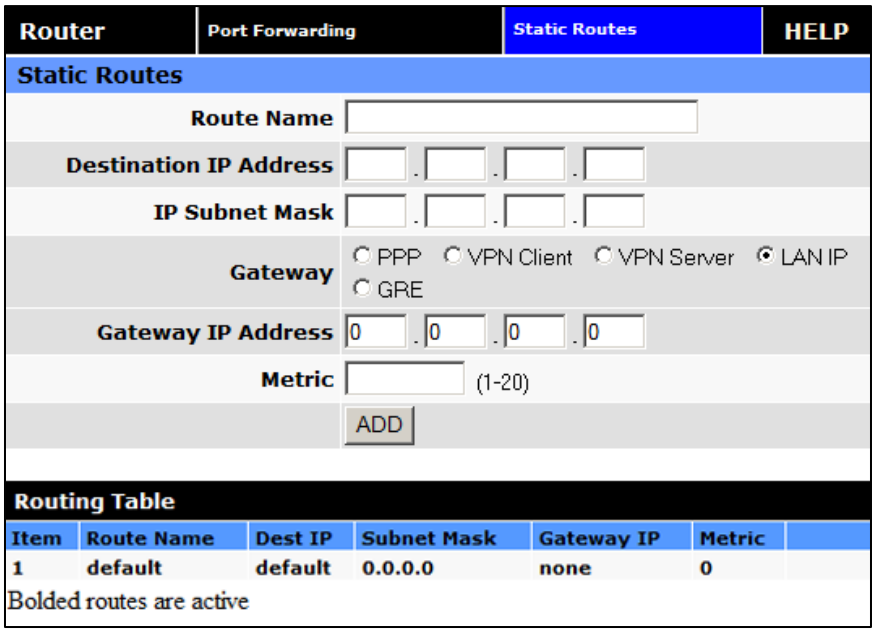
- **Destination Port**
  Sets the Local Area Network port number used when forwarding to the destination IP address.

Once you have completed the entry of the above fields, press the **ADD** button to save the new entry.

3.6.2 STATIC ROUTES

Select the **Static Routes** tab to open the routing configuration page. Static route tables may be created from the Routing screen and appear at the bottom. Static Routing refers to a manual method used to set up routing between networks.

Figure 28: Vanguard Router – Static Routes



Static Routes

- **Route Name**
  Sets the alphanumeric identifier of the static route in the Static Route Table

- **Destination IP Address**
  Sets the IP address of the destination network

- **IP Subnet Mask**
  Sets the subnet mask of the destination network

- **Gateway**
  Sets ppp (this router's wireless internet connection), pptp (VPN), GRE Tunnel, or the local network IP address for the gateway to the destination network

- **Gateway IP Address**
  This is only used if local IP addr was selected for gateway. Enter the address of the local gateway

- **Metric**
  Enter a number from 1 to 20. The lower the metric value the higher the route priority.

The **ADD** button must be pressed to add the configured route to the Static Route Table.

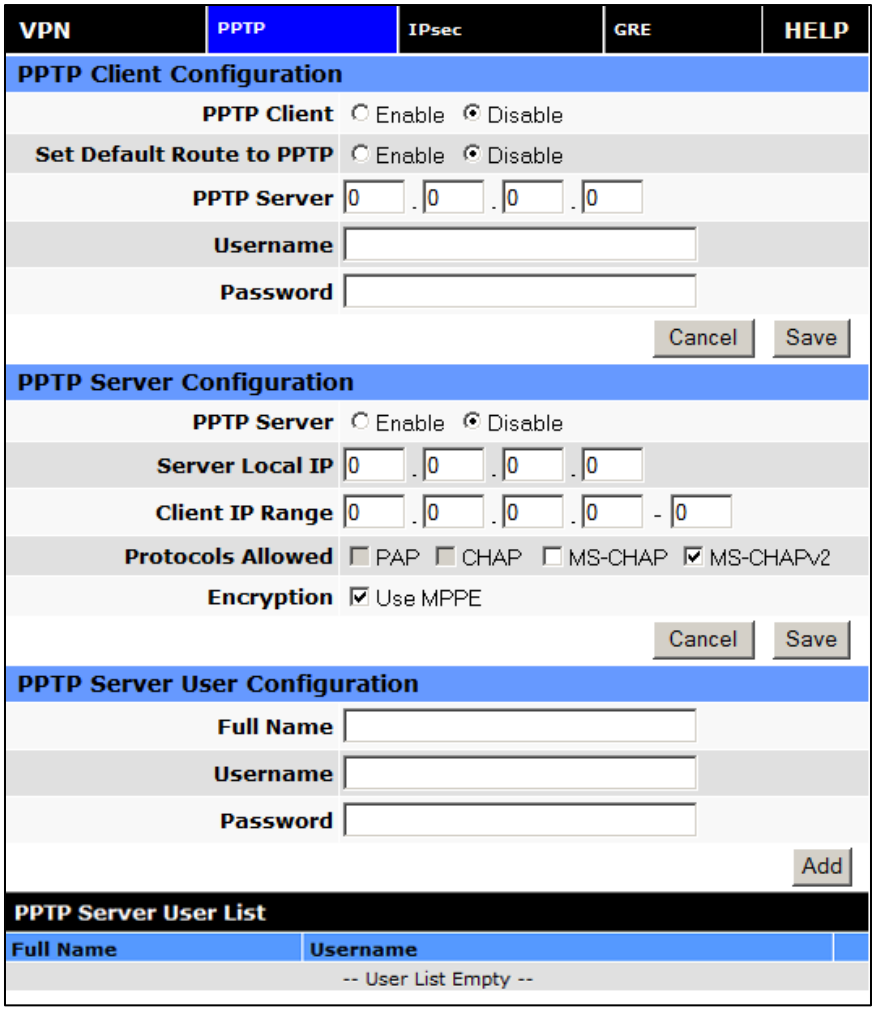
3.7 VPN

From the main navigation panel, select VPN for access to PPTP, IPsec and GRE screens.

3.7.1 PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPN).

Figure 29: Vanguard VPN – PPTP



PPTP Client Configuration

- **PPTP Client**
  Selecting Enable will allow the PPTP functionality. Selecting Disable will shut off PPTP functionality

- **Set Default Route to PPTP**
  Selecting Enable will route all IP traffic through the PPTP network. Selecting Disable will route only PPTP traffic through the PPTP network

- **PPTP Server**
  The IP address of the virtual private network server on which to connect

- **Username**
  The username required by the VPN server

- **Password**
  The password, associated with the username, required by the VPN server

PPTP Server Configuration

- **PPTP Server**
  Selecting Enable starts the VPN server, and selecting Disable stops it

- **Server Local IP**
  The IP address that clients will use to communicate with the server after they connect

- **Client IP Range**
  The pool of IP addresses assigned to clients

- **Protocols Allowed**
  Selecting a protocol will instruct the VPN server to accept clients who use that protocol. The server will reject clients using any of the un-selected protocols

- **Encryption**
  Selecting 'Use MPPE' will enable Microsoft Point-to-Point Encryption for communication between the server and clients. This option requires the MS-CHAP or MS-CHAPv2 protocol

PPTP Server User Configuration

- **Full Name**
  This name can be used as a more descriptive name for a client. It is not used by the server. No spaces are allowed in the name

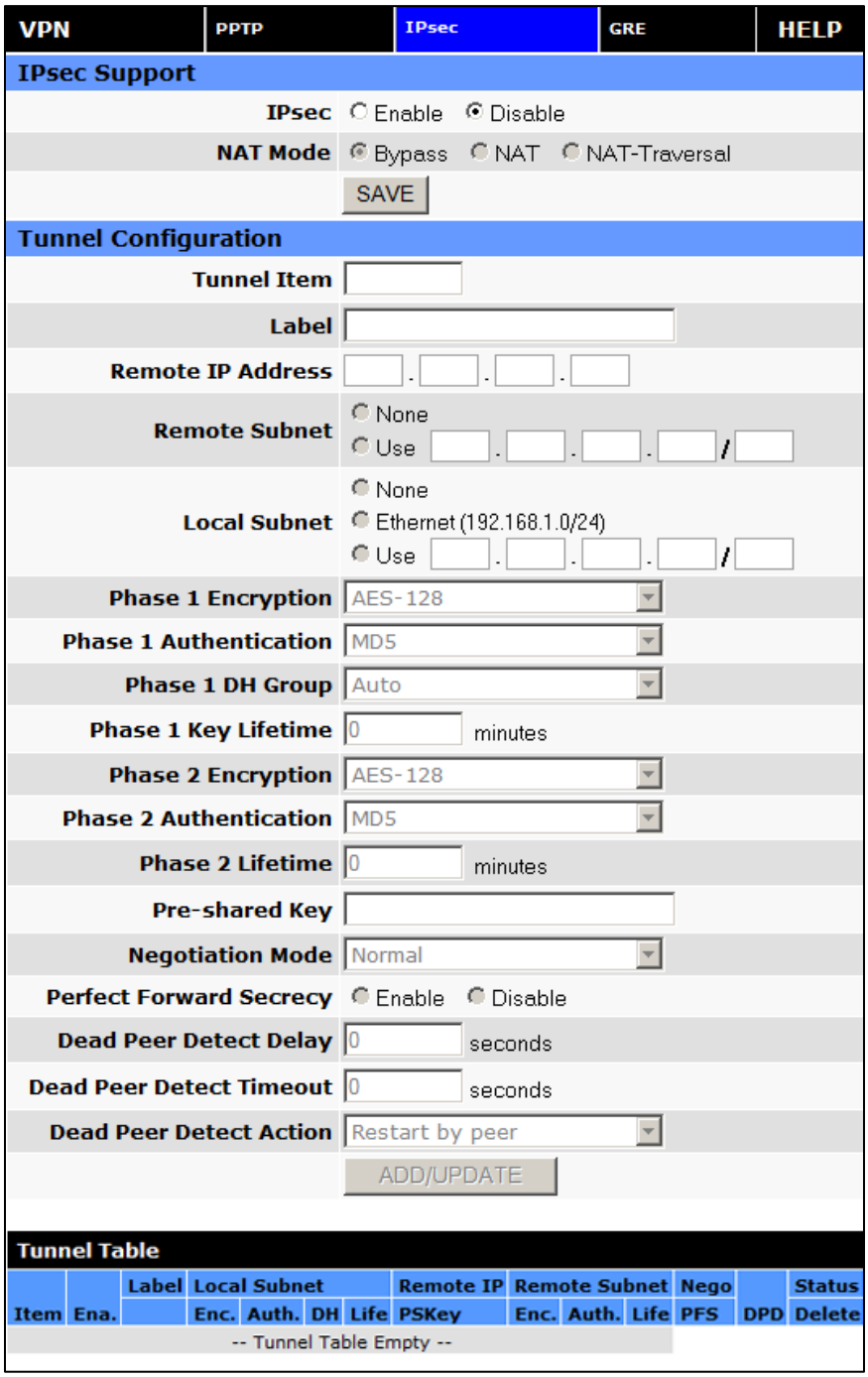
- **Username**
  The name used by a client to log in to the server

- **Password**
  The password, with associated username, used by a client to log in to the server

3.7.2 IPSEC

IPsec serves to configure secured communication tunnels. The various tunnel configurations will be displayed in the Tunnel Table at the bottom of the page. All tunnels are created using the ESP (Encapsulating Security Payload) protocol.

Figure 30: Vanguard VPN – IPSec



IPsec Support

- **IPsec**
  Selecting Enable will launch the IPsec process and start all enabled tunnels. Selecting Disable will stop all tunnels and shutdown the IPsec process. Note that all enabled tunnels will be launched automatically when the unit connects to the cellular carrier.

- **NAT Mode**
  Determines how packets are addressed. Selecting Bypass will allow packets coming from Local Subnet addresses through the NAT firewall unchanged. This may be sufficient when traffic only travels from Local Subnet to Remote Subnet. (LAN Settings > Bind to Eth IP may need to be enabled to make sure that packets generated by Vanguard services appear to originate from a Local Subnet address.) NAT changes the source address to match the Status > PPP IP Address. NAT-Traversal enables the NAT-T protocol which can support traffic beyond just the Local & Remote Subnets.

Tunnel Configuration

- **Tunnel Item**
  Tunnel number, starts from 1 and increments for each new tunnel. To update an existing tunnel, use its corresponding number from the tunnel table. To add a new tunnel, use the last tunnel shown in the Tunnel Table + 1.

- **Label**
  This is a label to identify a tunnel and must correspond to the name specified for the remote endpoint.

- **Remote IP Address**
  The IP address of the remote endpoint of the tunnel.

- **Remote Subnet**
  Choose None if encrypted packets are only destined for the Remote IP Address. Use an IP address / mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address. **IMPORTANT: The Remote Subnet and Local Subnet addresses must not overlap!**

- **Local Subnet**
  Choose None if only packets generated by Vanguard services will be sent over the tunnel. Choose Ethernet if packets from the local LAN will also be sent over the tunnel. (LAN Settings > Bind to Eth IP may need to be enabled to make sure that packets generated by Vanguard services appear to originate from a Local Subnet address.) Use an IP address / mask if a network beyond the local LAN will be sending packets over the tunnel. **IMPORTANT: The Remote Subnet and Local Subnet addresses must not overlap!**

- **Phase 1 Encryption**
  Use AES-128, AES-256 or 3DES encryption.

- **Phase 1 Authentication**
  Use MD5 or SHA1 hashing.

- **Phase 1 DH Group**
  Negotiate (Auto) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) bit keys.

- **Phase 1 Key Lifetime**
  How long the keying channel of a connection should last before being renegotiated.

- **Phase 2 Encryption**
  Use AES-128, AES-256 or 3DES encryption.

- **Phase 2 Authentication**
  Use MD5 or SHA1 hashing.

- **Phase 2 Lifetime**
  How long a particular instance of a connection should last, from successful negotiation to expiry.

- **Pre-shared Key:**
  Predetermined key known to both the local unit and the remote side prior to establishing the tunnel.

- **Negotiation Mode**
  Choose Normal to allow IPsec to negotiate some connection parameters. Choose Aggressive to require that only those parameters selected above can be used to create the tunnel.

- **Perfect Forward Secrecy**
  Enable Perfect Forward Secrecy for the session keys.

- **Dead Peer Detection Delay**
  Tunnel keepalive time for R_U_THERE packets during idle periods.

- **Dead Peer Detection Timeout**
  Timeout time during tunnel idle periods where no R_U_THERE_ACK has been received.

- **Dead Peer Detection Action**
  Action to be taken when timeout value is reached.

Once you have completed the entry of the above fields, press the **ADD/UPDATE** button to save the new entry.

Tunnel Table

- **Enable**
  Check Ena to enable a tunnel. The tunnel's state is saved across resets

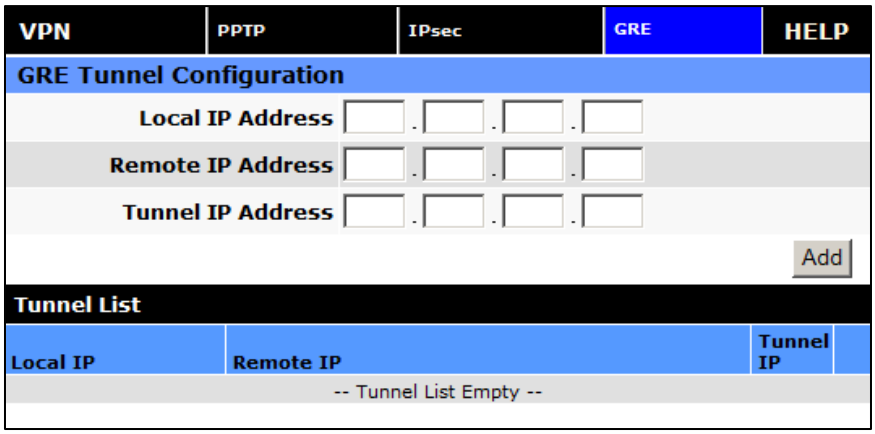
- **View**
  Click on View to open a page showing the log of the tunnel's negotiation activity

- **Delete**
  Click on Del to delete the tunnel

3.7.3 GRE

The GRE screen is used to add and delete GRE tunnels. Current tunnels are listed below. Static routes may be necessary to route desired traffic through a particular tunnel.

Figure 31: Vanguard VPN – GRE



GRE Tunnel Configuration

- **Local IP Address**
  The local IP address associated with the tunnel

- **Remote IP Address**
  The remote IP address associated with the tunnel

- **Tunnel IP Address**
  The IP address assigned to the tunnel interface.

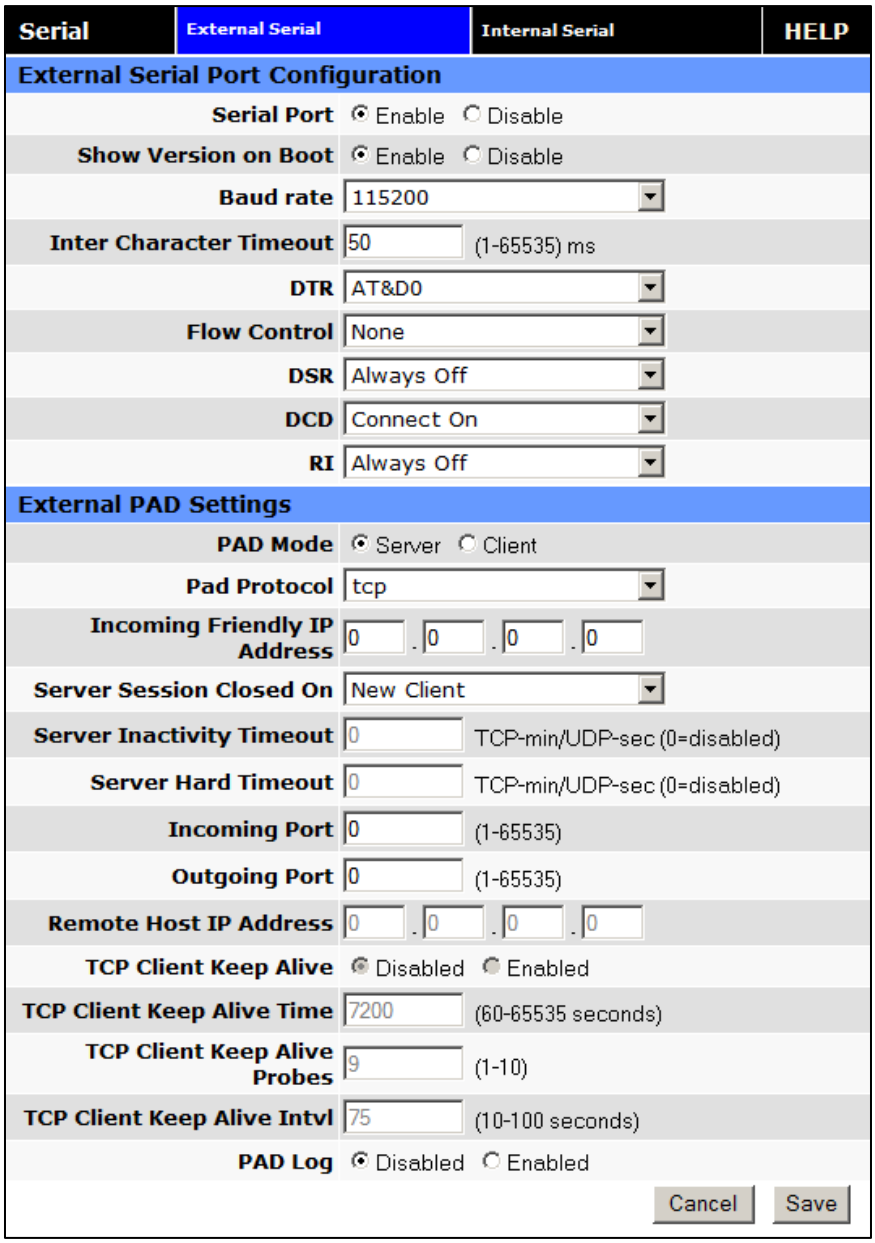
3.8 SERIAL

From the main navigation pane, select Serial for access to both external and internal serial port configuration screens.

3.8.1 EXTERNAL SERIAL

The External Serial screen is used to configure the RS-232 Serial Port parameters and Packet Assembler and Disassembler (PAD) functionality. The PAD feature forwards requests that come in on a specific port to the Serial connector.

Figure 32: Vanguard Serial – External Serial



External Serial Port Configuration

- **Serial Port**
  When enabled, the external serial port PAD function can be used. When disabled, no PAD function is available, and the port is left free, for use by an ODP application.

- **Show Version on Boot**
  When enabled, the router model number and firmware version are transmitted out the serial port at router boot. Additionally, "OK" is transmitted when router is ready to receive data and when PPP connection is made. When disabled, these indicators will not be transmitted out the serial port.

- **Baud Rate**
  Sets the baud rate of the serial port. Settings may range from 300 to 115,200 bits per second. The default baud rate is 115,200 bps.

- **Inter Character Timeout**
  Sets the Inter Character Timeout from 1 to 65,535 ms.

- **DTR**
  Defines the Data Terminal Ready behavior. Refer to Table XX for DTR descriptions.

Table 7 – DTR Descriptions

AT&D0	Ignore DTR.
AT&D1	If in the Online Data State, upon an on-to-off transition of DTR, the modem enters Online Command State and issues an OK result code; the call remains connected. Otherwise, ignore DTR.
AT&D2	If in the Online Data State or Online Command State upon an on-to-off transition of DTR, the modem performs an orderly clear-down of the call and returns to the command state. Automatic answer is disabled while DTR remains off.
AT&D4	The modem auto-dials the default remote station upon an off-to-on transition of DTR and enters the Online Data State. The modem ends the call and enters the command state upon an on- to-off transition of DTR.
AT&D5	The modem auto-dials the default remote station upon an on-to-off transition of DTR and enters the Online Data State. The modem ends the call and enters the command state upon an off-to-on transition of DTR.
AT&D6	Upon an on-to-off transition of DTR, the modem performs an orderly clear-down of any session and turns OFF the RF module. Upon an off-to-on transition of DTR, the modem turns ON the RF module and reestablishes the radio session.
AT&D7	Upon an on-to-off transition of DTR, the modem performs an orderly clear-down of any session and turns OFF the RF module. Upon an off-to-on transition of DTR, the modem turns ON the RF module and reestablishes the radio session.
AT&D8	The modem auto-dials the default remote station upon determining DTR is OFF and enters the Online Data State. The modem ends the call and enters the command state upon determining DTR is ON.
AT&D9	The modem auto-dials the default remote station upon determining DTR is ON and enters the Online Data State. The modem ends the call and enters the command state upon determining DTR is OFF.

- **Flow Control**
  Sets the Flow Control to None or Hardware control

- **DSR**
  Sets the Data Set Ready to Always On, On When Available, On When Connected or Always Off. The DSR parameter determines how the modem controls the state of the Data Set Ready circuit. The default value is Always Off.
  - Always On: DSR is always on.
  - On When Available: DSR is on when the RF signal present and phone registered on network.
  - On When Connected: DSR is on when connected to CDMA.
  - Always Off: DSR is always off.

- **DCD**
  The DCD parameter determines how the modem controls the state of the Carrier Detect circuit and the amber DCD LED on the front panel. The default value is Connect On.
  - Always On: DCD is always on.
  - Connect On: DCD is on when connected to a remote host.
  - Always Off: DCD is always off.

- **RI**
  The RI parameter determines how the modem controls the state of the Ring Indicator circuit. The default value is Always Off.
  - Always On: RI is always on.
  - Connect On: RI tracks incoming ring pulse.
  - Always Off: RI is always off.

External PAD Settings

- **PAD Mode**
  Select button to set the PAD mode of the modem as a Server or Client. In Client mode, the modem will initiate an outbound connection to the Remote Host IP Address with the Outgoing Port based on the selected DTR setting. In Server mode, the modem will accept one incoming connection on the specified Incoming Port. The modem will not accept multiple incoming connections at the same time – additional connections are arbitrated based on the Server Session Closed On and Timeout parameters. Note: It is possible to override Server mode and make an outgoing client connection using the RS-232 command set.

  atd*xxx.xxx.xxx.xxx:yyyyy – When in server mode, and no connection is active, the atd* command (followed by an IP address) can be issued to initiate an outbound client connection to the specified IP address and port as specified after the colon. If no port is specified, the port number used is the Outgoing Port parameter. To hang-up such a connection, 3 '+' characters must be inserted into the outgoing stream ("+++"). The modem will return to command mode once it has seen the "+++" and respond with OK. The connection can then be broken by entering "ath". The modem will return to server mode. Such a client connection can be repeated again as necessary, as long as each connection is hung-up before a new one is made.

  Additional note: The modem is capable of only 1 PAD connection at a time. When a manual client connection is in progress (atd*xxx.xxx.xxx.xxx), a connection attempt by an incoming client may result in the disabling of the PAD function until the next device reset.

- **Pad Protocol**

  Sets the data protocol of the PAD to tcp or udp data. If you have set PAD Mode as server you can choose either to support either type of client.

- **Incoming Friendly IP Address**
  Sets the IP address of the device using the PAD functionality

- **Server Session Closed On**
  This is only available if PAD mode is Server. This option selects under which condition the server will terminate an established connection.

New Client: If a different client attempts to connect, it will be successful and the current client will be forcibly disconnected, without any warning. Otherwise, the current client remains connected indefinitely.

Timeout: A new client will be accepted only after a specified timeout. The duration of the timeout is specified by the Inactivity timeout, or the Hard timeout, or a combination of both.

The default value is New Client.

- **Server Inactivity Timeout**
  Time after which the current connection with Client will be terminated without warning. This time starts over again each time the Client sends data to the server. This parameter is ignored if the session closes on New Client. If PAD protocol is tcp, the timeout is specified in minutes. If UDP, the timeout is specified in seconds. The valid range for either is 1-65535. 0 will disable this timer.

  If both Inactivity Timeout and Hard Timeout are enabled, (neither is 0), then a client session will be terminated when either timeout is met. In this case, the value for Hard Timeout must exceed the value for Inactivity Timeout. If the Inactivity Timeout is met, the client will be terminated. If the Hard Timeout is exceeded without meeting the Inactivity Timeout, the client will be terminated by the Hard Timeout.

- **Server Hard Timeout**
  Time after which the current connection with Client will be terminated without warning. This is a fixed time from the initial connection, no matter how much or how often the Client sends data to the server. This parameter is ignored if the session closes on New Client. If PAD protocol is tcp, the timeout is specified in minutes. If udp, the timeout is specified in seconds. The valid range for either is 1-65535. 0 will disable this timer.

  If both Inactivity Timeout and Hard Timeout are enabled, (neither is 0), then a client session will be terminated when either timeout is met. In this case, the value for Hard Timeout must exceed the value for Inactivity Timeout. If the Inactivity Timeout is met, the client will be terminated. If the Hard Timeout is exceeded without meeting the Inactivity Timeout, the client will be terminated by the Hard Timeout.

- **Incoming Port**
  Sets the port number used to forward incoming requests to the serial port

- **Outgoing Port**
  Sets the port number used to send outgoing requests from the serial port

- **Remote Host IP Address**
  Sets the Server IP address to connect with when using the PAD in client mode

- **TCP Client Keep Alive**
  When in client mode and enabled, TCP Keep Alive packets will be sent from the client to the server periodically in order to detect a broken connection. The modem will automatically try to re-establish the connection if necessary. Changing this setting will affect the use of TCP Keep Alive on the next client session. It will not affect an existing session

- **TCP Client Keep Alive Time**

Time in seconds between keep alive cycles. A keep alive cycle will consist of one or more keep alive probes separated by the keep alive interval.

- **TCP Client Keep Alive Probes**
  Number of keep alive packets that must fail before connection is considered closed

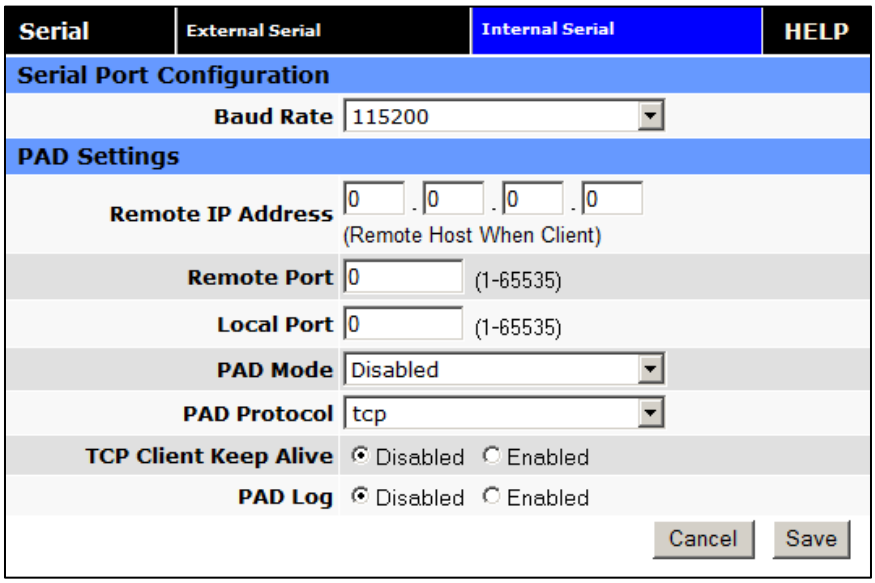
- **TCP Client Keep Alive Intvl**
  Time in seconds after which a keep alive packet is considered to be failed (if not acknowledged). Another packet is sent at this time if TCP Client Keep Alive Probes limit has not been reached

- **PAD Log**
  When enabled, as data passes through the PAD, a copy is stored in a log file located on the modem at /tmp/padlog. The log will stop saving data when full and data is lost at modem reset.

3.8.2 INTERNAL SERIAL

The Internal Serial screen is used to configure the internal RS232 Serial Port parameters and Packet Assembler and Disassembler (PAD) functionality. The PAD feature forwards requests that come in on a specific port to the internal serial port.

Figure 33: Vanguard Serial – Internal Serial



Serial Port Configuration

- **Baud Rate**
  Sets the baud rate of the serial port. Settings may range from 300 to 115,200 bits per second. The default baud rate is 115,200 bps.

PAD Settings

- **Remote IP Address**
  Sets the IP address of the device using the PAD functionality

- **Remote Port**
  Sets the port number used by the remote device to accept requests from the Vanguard

- **Local Port**
  Sets the port number used by the Vanguard to accept requests from the remote device

- **PAD Mode**
  Select buttons to set the PAD mode of the Vanguard as a Server or Client

- **Pad Protocol**
  Sets the data protocol of the PAD to tcp or udp data

- **TCP Client Keep Alive**
  When in client mode and enabled, TCP Keep Alive packets will be sent from the client to the server periodically in order to detect a broken connection. The modem will automatically try to re-establish the connection if necessary. Changing this setting will affect the use of TCP Keep Alive on the next client session. It will not affect an existing session. When this option is enabled, the timing and number of Keep Alive attempts is controlled by parameters defined on the External Serial page. It is not possible to have different timing settings for each serial port

- **PAD Log**
  If enabled, a log of the data passed through the modem is saved at /tmp/intpadlog. The log will stop saving data when full and data is lost at modem reset.

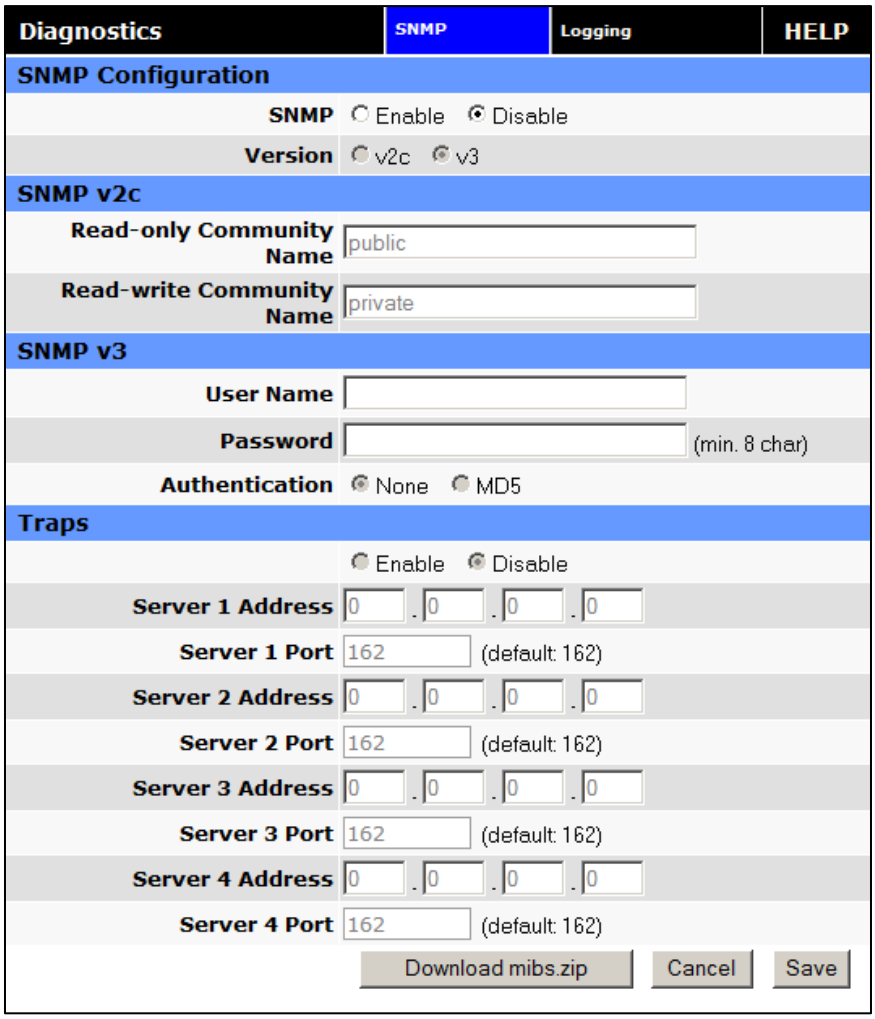
3.9 DIAGNOSTICS

From the main navigation pane, select Diagnostics for access to the SNMP and Logging screens.

3.9.1 SNMP

The Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP version v2c and v3 are supported with the exception of INFORM.

Figure 34: Vanguard Diagnostics – SNMP



SNMP Configuration

- **SNMP**
  Selecting Enable will allow the SNMP functionality. Selecting Disable will shut off SNMP functionality.

- **Version**
  With SNMP Enabled, select the corresponding version that matches the SNMP Manager.

SNMP v2c

- **Read-only Community Name**
  The community string used for accessing the read-only Management Information Bases (MIBs)

- **Read-write Community Name**
  The community string used for accessing all Management Information Bases (MIBs) including writable objects

SNMP v3

- **User Name**
  The user name for secure access to the Management Information Bases (MIBs) observing v3 standard

- **Password**
  The corresponding user password for accessing the Management Information Bases (MIBs) including writable objects

- **Authentication**
  Selecting the authentication method for accessing the Management Information Bases (MIBs)

Traps

- **Traps**
  Selecting Enable will allow the active trap events to be reported to the defined server(s). Selecting Disable will desactivate events reporting. Up to four destinations can be specified.

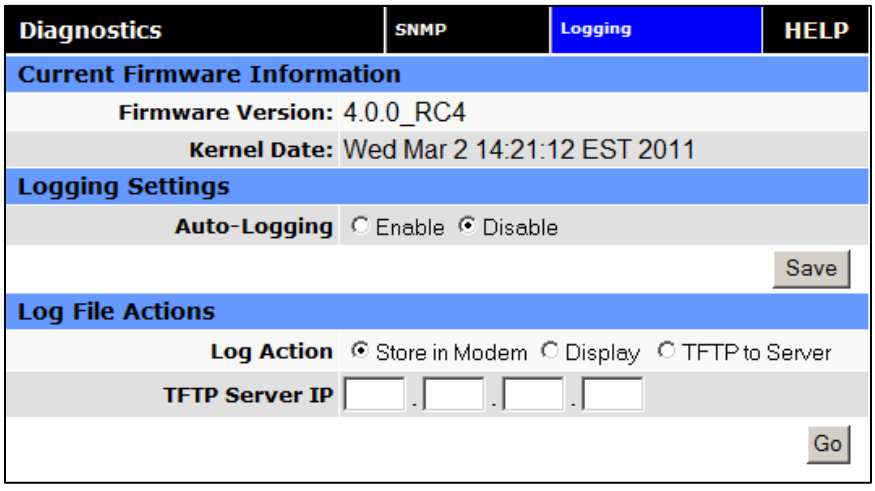
- **Server Address**
  IP address of server to which the trap events will be sent to.

- **Server Port**
  The corresponding server port to which the trap events will be sent to (default 162).

3.9.2 LOGGING

The Logging screen provides a way to capture the current status log of the modem. Log information is useful when contacting CalAmp Technical Support to resolve operational problems.

Figure 35: Vanguard Diagnosics – Logging



Current Firmware Information

- **Version**
  Displays the modem firmware version currently loaded in the unit

- **Kernel Date**
  Displays the date of the operating system kernel the unit is running

Logging Settings

- **Auto-Logging**
  Selecting Enable and pressing Save will enable the logging capability which saves periodic and event driven logs to permanent memory. Technical Services personnel may find such logs useful in analyzing field issues. Selecting Disable and pressing Save will disable the logging capability. This is the default setting. To make best use of available memory it is recommended to only enable the logging capability if it is necessary to help diagnose an issue.

Log File Actions

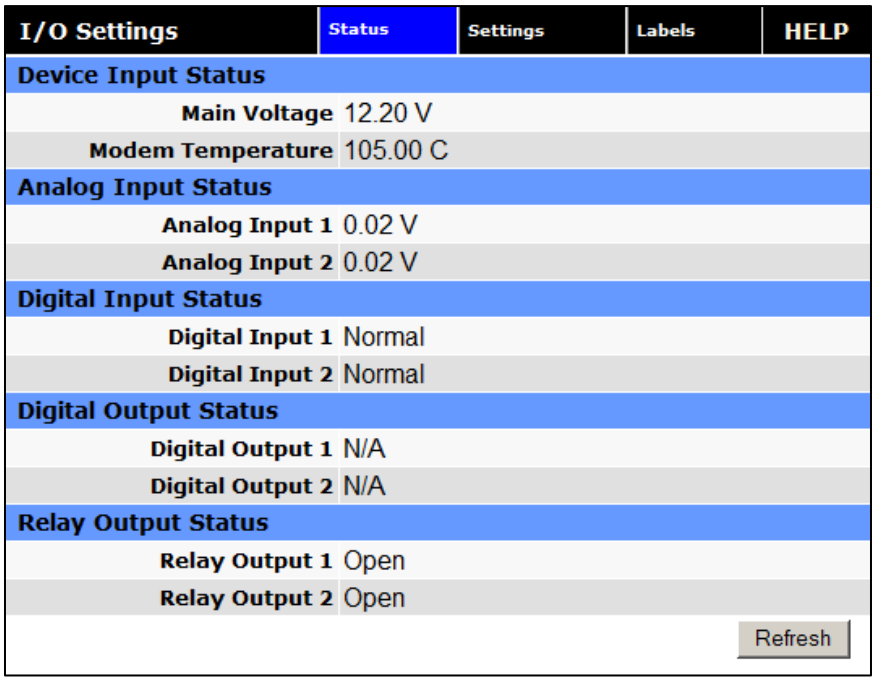
- **Log Action**
  - Store in modem: Selecting Store in Modem and pressing Go will create a current status log, and overwrite any previously saved log. This action will save a log even if auto-logging is disabled. It is best to save the log immediately following the adverse event, and before any reboot. This log will contain only information collected since the most recent reboot of the device.
  - Display: Selecting Display and pressing Go will display a previously stored log directly to the web browser. You can use your mouse to select the text, copy it, and paste it into a text editor to save the log on your computer.
  - TFTP to Server: Selecting TFTP to Server and pressing Go will initiate a transfer of a previously saved log file to a specified IP address using the TFTP protocol. In order for the transfer to be successful, a reachable IP address must be entered under TFTP Server IP and the computer at that IP address must be running a TFTP Server program. Many free TFTP Servers are available for download over the internet. Note that TFTP is different than FTP.

- **TFTP Server IP**
  When selecting TFTP to Server and pressing Go a valid and reachable IP address must be entered here in order to complete the transfer of the saved log file using the TFTP protocol. In order for the transfer to be successful, a reachable IP address must be entered under TFTP Server IP and the computer at that IP address must be running a TFTP Server program. Many free TFTP Servers are available for download over the internet. Note that TFTP is different than FTP.

3.10 I/O SETTINGS

3.10.1 STATUS

Figure 36: Vanguard I/O Settings – Status



Device Input Status

- **Main Voltage**
  Displays current voltage applied to the unit, in Volts

- **Modem Temperature**
  Displays temperature of the Wireless Modem, in Celsius

Analog Input Status

- **Analog Input 1, Analog Input 2**
  Displays voltage of the specified analog input, in Volts.

Digital Input Status

- **Digital Input 1, Digital Input 2**
  Displays the status of the specified input: Active (high state) or Normal (low state)

Digital Output Status

- **Digital Output 1, Digital Output 2**
  Currently Not Available

Relay Output Status

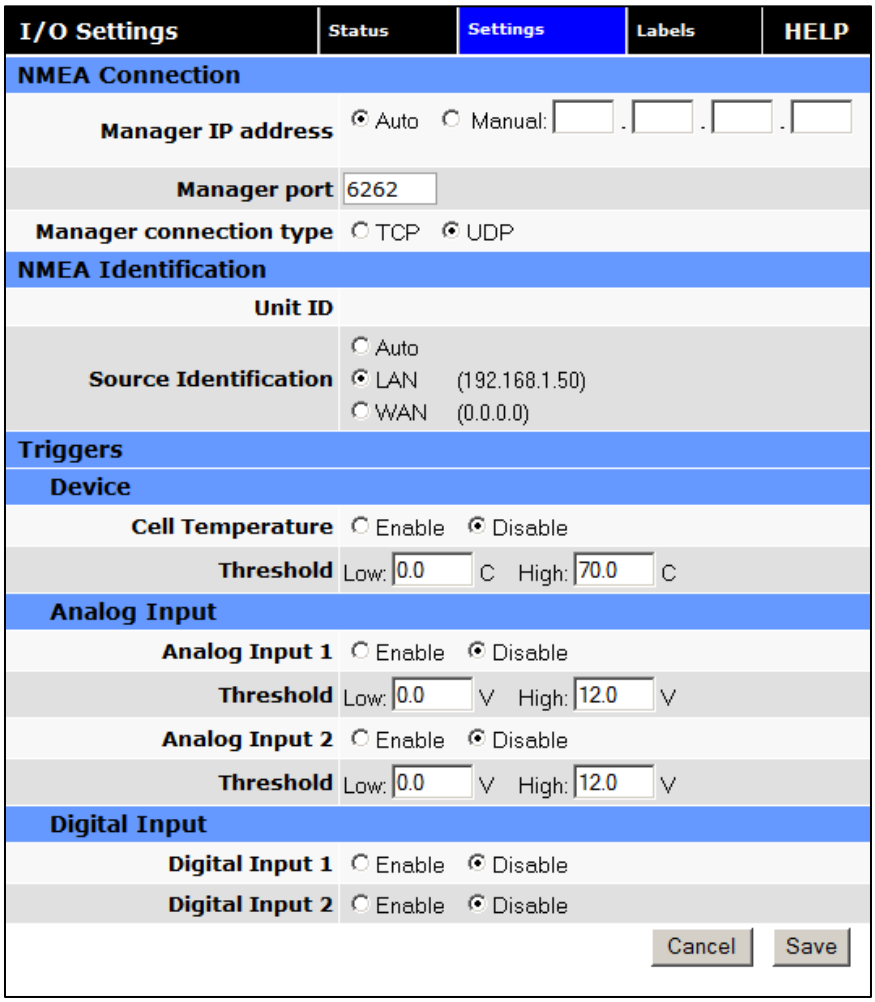
- **Relay Output 1, Relay Output 2**

Displays the status of the specified output as open or closed

3.10.2 SETTINGS

Status Monitoring is provided via NMEA-based protocol. The Vanguard I/O subsystem operates according to a manager/agent model. The PC-hosted manager sends requests to the Vanguard I/O agent, which performs the required actions. The Vanguard agent reports alarms to the PC-hosted manager.

Figure 37: Vanguard I/O Settings – Settings



NMEA Connection

- **Manager IP address/port**
  The IP address and service port of the NMEA server (manager)

- **Manager connection type**
  The connection protocol to communicate with the NMEA server (manager)

NMEA Identification

- **Unit ID**
  The Unit Name to be included in the NMEA message payload.

- **Source Identification**
  The Unit's IP address that will be included in the NMEA message payload

Triggers – Device

- **Cell Temperature and thresholds**
  Enable or disable NMEA alarm and notification when temperature goes out of range.

Triggers – Analog Input

- **Analog Input and thresholds (1 or 2)**
  Enable or disable NMEA alarm and notification when an analog input goes out of range.

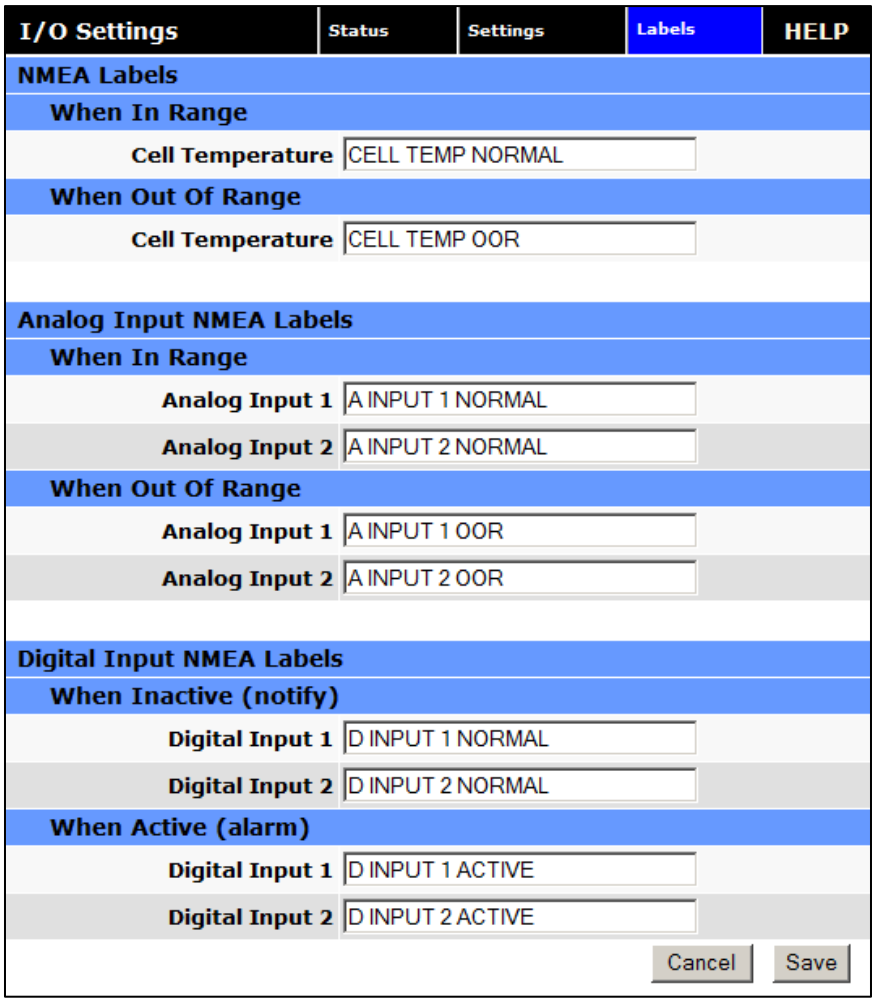
Triggers – Digital Input

- **Digital Input 1, Digital Input 2**
  Enable or disable NMEA alarm and notification when the input state changes.

3.10.3 LABELS

Each diagnostic value can be user-defined messages indicating its normal and abnormal conditions.

Figure 38: Vanguard I/O Settings – Labels



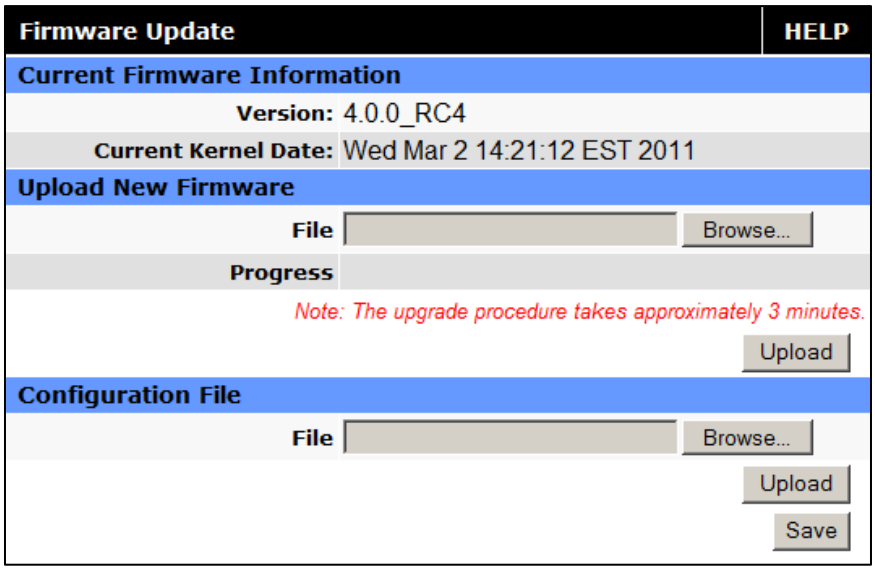
3.11 FIRMWARE UPDATE

When newer versions of the modem firmware become available, the user can download the proper file from the CalAmp web site and manually update the unit by uploading the new firmware.

The update file name is:

- upgradeevdo.tar.gz for the Vanguard EVDO modem.

Figure 39: Vanguard Firmware Update



Current Firmware Information

- **Version**
  Displays the modem firmware version currently loaded in the unit.

- **Kernel Date**
  Displays the date of the operating system kernel the unit is running

Upload New Firmware

- **File**
  Enter the update file name or you may use the browse button to locate the file from your hard drive. Updates can be done if Remote Administration is enabled.

- **Progress**
  Displays the update progress after the Save button has been pressed.

- **Upload Button**
  After selecting the firmware upgrade filename above, press the Upload button to begin the firmware upgrade process.

Configuration File

- **File**
  Field to input the uploaded configuration file to the modem. The Browse button can be used to locate the file in a specific folder. The file to be uploaded must be named config.xml. If multiple files need to be maintained, it is recommended that separate directories be used. The update can be done remotely if Remote Administration is enabled.

- **Upload Button**
  After selecting the firmware configuration filename above, press the Upload button to begin the configuration loading process.

- **Save**
  Returns a link to the configuration file on the unit. Right-click the link and select "Save Target As..." to save the file. The link page refreshes after 15 seconds. It is recommended to use the specified filename to save the file. If multiple files need to be maintained, it is recommended to use directory paths to separate the files.

4 SERVICE AND SUPPORT

Product Warranty, RMA and Contact Information

CalAmp guarantees that every Vanguard Modem will be free from physical defects in material and workmanship for one (1) year from the date of purchase when used within the limits set forth in the Specifications section of this manual.

The manufacturer's warranty statement is available in Appendix 1. If the product proves defective during the warranty period, contact CalAmp Customer Service to obtain a Return Material Authorization (RMA).

RMA Request/Contact Customer Service

CalAmp
299 Johnson Avenue, Suite 110
Waseca, MN 56093
Tel: 507-833-8819 ext. 6707
Fax: 507-833-6748

BE SURE TO HAVE THE EQUIPMENT MODEL AND SERIAL NUMBER, AND BILLING AND SHIPPING ADDRESSES ON HAND WHEN CALLING.

When returning a product, mark the RMA clearly on the outside of the package. Include a complete description of the problem and the name and telephone number of a contact person. RETURN REQUESTS WILL NOT BE PROCESSED WITHOUT THIS INFORMATION.

For units in warranty, customers are responsible for shipping charges to CalAmp. For units returned out of warranty, customers are responsible for all shipping charges. Return shipping instructions are the responsibility of the customer.

Product Documentation

CalAmp reserves the right to update its products, software, or documentation without obligation to notify any individual or entity. Product updates may result in differences between the information provided in this manual and the product shipped. For the most current product documentation, visit www.calamp.com for datasheets, programming software and user manuals.

Technical Support

CalAmp
299 Johnson Avenue, Suite 110
Waseca, MN 56093
Tel: 507-833-8819
E-mail: wngsupport@calamp.com

APPENDIX A – ABBREVIATIONS

Abbreviation	Description
APN	Access Point Name
CSD	Circuit Switched Data
CTS	Clear to Send
DCD	Data Carrier Detect
DCE	Data Communication Equipment
DTE	Data Terminal Equipment
IMEI	International Mobile Equipment Identity
EDGE	Enhanced Data rates for Global Evolution
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communication
HSDPA	High-Speed Downlink Packet Access
LED	Light Emitting Diode
ME	Mobile Equipment
MS	Mobile Station
OTA	Over the Air
PDP	Packet Data Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PRL	Preferred Roaming List
RSSI	Receive Signal Strength Indication
Rx	Receive
Tx	Transmit

APPENDIX B – WARRANTY STATEMENT

CalAmp warrants to the original purchaser for use ("Buyer") that data telemetry products manufactured by Dataradio ("Products") are free from defects in material and workmanship and will conform to published technical specifications for a period of, except as noted below, one (1) year from the date of shipment to Buyer. CalAmp makes no warranty with respect to any equipment not manufactured by Dataradio, and any such equipment shall carry the original equipment manufacturer's warranty only. CalAmp further makes no warranty as to and specifically disclaims liability for, availability, range, coverage, grade of service or operation of the repeater system provided by the carrier or repeater operator. Any return shipping charges for third party equipment to their respective repair facilities are chargeable and will be passed on to the Buyer.

If any Product fails to meet the warranty set forth above during the applicable warranty period and is returned to a location designated by CalAmp. CalAmp, at its option, shall either repair or replace such defective Product, directly or through an authorized service agent, within thirty (30) days of receipt of same. No Products may be returned without prior authorization from CalAmp. Any repaired or replaced Products shall be warranted for the remainder of the original warranty period. Buyer shall pay all shipping charges, handling charges, fees and duties for returning defective Products to CalAmp or authorized service agent. CalAmp will pay the return shipping charges if the Product is repaired or replaced under warranty, exclusive of fees and duties. Repair or replacement of defective Products as set forth in this paragraph fulfills any and all warranty obligations on the part of CalAmp.

This warranty is void and DRL shall not be obligated to replace or repair any Products if (i) the Product has been used in other than its normal and customary manner; (ii) the Product has been subject to misuse, accident, neglect or damage or has been used other than with CalAmp approved accessories and equipment; (iii) unauthorized alteration or repairs have been made or unapproved parts have been used in or with the Product; or (iv) Buyer failed to notify CalAmp or authorized service agent of the defect during the applicable warranty period. DRL is the final arbiter of such claims.

THE AFORESAID WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED AND IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. DRL AND BUYER AGREE THAT BUYER'S EXCLUSIVE REMEDY FOR ANY BREACH OF ANY OF SAID WARRANTIES IT AS SET FORTH ABOVE. BUYER AGREES THAT IN NO EVENT SHALL DRL BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT OR EXEMPLARY DAMAGES WHETHER ON THE BASIS OF NEGLIGENCE, STRICT LIABILITY OR OTHERWISE. The purpose of the exclusive remedies set forth above shall be to provide Buyer with repair or replacement of non-complying Products in the manner provided above. These exclusive remedies shall not be deemed to have failed of their essential purpose so long as DRL is willing and able to repair or replace non-complying Products in the manner set forth above.

This warranty applies to all Products sold worldwide. Some states do not allow limitations on implied warranties so the above limitations may not be applicable. You may also have other rights, which vary from state to state.

EXCEPTIONS

THIRTY DAY:	Tuning and adjustment of telemetry radios
NO WARRANTY:	Fuses, lamps and other expendable parts